Estratégia
CONCURSOS

Aul

Computação Forense para Concursos (Área de TI) - Curso Regular - 2020

Professor: Equipe Informática e TI, Evandro Dalla Vecchia Pereira

Sumário

Apresentação do Curso 3

Apresentação Pessoal 3

PARE TUDO! E preste atenção!! 4

Cronograma de Aulas 5

Introdução ao Estudo da Computação Forense 6

1 - Considerações Iniciais 6

2 - Crimes Eletrônicos 6

2.1 – Conceitos 6

2.2 – Questões Comentadas 10

3 - Engenharia Social 14

3.1 – Conceitos 14

3.2 – Questões Comentadas 14

4 - Phishing 18

4.1 – Conceitos 18

4.2 – Questões Comentadas 19

5 - Pharming 23

5.1 – Conceitos 23

5.2 – Questões Comentadas 26

6 - Sniffer 32

6.1 – Conceitos 32

6.2 – Questões Comentadas 34

7 - Negação de Serviço (DoS/DDoS) 41

7.1 – Conceitos 41

7.2 – Questões Comentadas 42

8 - Softwares Maliciosos (Malwares) 47

8.1 – Conceitos 47

8.2 – Questões Comentadas 53

Lista de Questões 61

Gabarito 87

APRESENTAÇÃO DO CURSO

Iniciamos nosso curso em teoria e questões. As aulas em PDF possuem por característica essencial a didática. Ao contrário do que encontramos em alguns livros, o curso todo se desenvolverá com uma leitura de fácil compreensão e assimilação.

Além disso, teremos videoaulas! Essas aulas destinam-se a complementar a preparação. Quando estiver cansado do estudo ativo (leitura e resolução de questões) ou até mesmo para a revisão, abordaremos alguns pontos da matéria por intermédio dos vídeos. Com outra didática, você disporá de um conteúdo complementar para a sua preparação. Ao contrário do PDF, evidentemente, AS VIDEOAULAS NÃO ATENDEM A TODOS OS PONTOS QUE VAMOS ANALISAR NOS PDFS, NOSSOS MANUAIS ELETRÔNICOS. Por vezes, haverá aulas com vários vídeos; outras que terão videoaulas apenas em parte do conteúdo. Nosso foco é sempre o estudo ativo!

APRESENTAÇÃO PESSOAL

Meu nome é Evandro Dalla Vecchia Pereira, sou autor do livro "Perícia Digital - Da investigação à análise forense", Mestre em Ciência da Computação (UFRGS), Bacharel em Ciência da Computação (PUCRS), Técnico em Redes de Computadores (Etcom/UFRGS) e em Processamento de Dados (Urcamp). Perito Criminal na área de Perícia Digital desde 2004 no Instituto-Geral de Perícias/RS. Professor de pós-graduação em diversas instituições, nas áreas de Perícia Digital, Perícia Criminal e Auditoria de Sistemas. Lecionei em cursos de graduação de 2006 a 2017, nas instituições PUCRS, Unisinos, entre outras e sou professor em cursos de formação e aperfeiçoamento de Peritos Criminais, Delegados, Inspetores, Escrivães e Policiais Militares.

No Estratégia Concursos leciono desde o começo de 2018, inicialmente na área de Computação Forense e, na sequência, também assumi as áreas de Arquitetura de Computadores e Sistemas Operacionais, tanto na elaboração de materiais escritos como na gravação das videoaulas.

Deixarei abaixo meus contatos para quaisquer dúvidas ou sugestões. Terei o prazer em orientá-los da melhor forma possível nessa caminhada que estamos iniciando.

Instagram: @profevandrodallavecchia
Facebook: https://www.facebook.com/profevandrodallavecchia

Conte comigo! Grande abraço!

PARE TUDO! E PRESTE ATENÇÃO!!

Hoje eu faço parte de uma equipe SENSACIONAL de professores! Depois de muita luta conseguimos reunir um time de profissionais extremamente QUALIFICADO e sobretudo COMPROMISSADO em fazer o melhor pelos alunos. Para tal criamos um conjunto de ações para nos aproximarmos dos alunos, entendermos suas necessidades e evoluirmos nosso material para um patamar ainda mais diferenciado. São 3 as novidades que gostaria de convidá-lo a conhecer:



Nosso podcast alternativo ... livre, descontraído e com dicas rápidas que todo CANETA PRETA raiz deve ouvir. Já temos alguns episódios disponíveis e vários outros serão gravados nas próximas semanas ... acompanhe em:

http://anchor.fm/estrategia-tech



Nosso grupo do Telegram é um local onde ouvimos os alunos e trocamos ideias com eles. Está crescendo a cada dia. A regra do grupo é: só vale falar sobre concursos. Lá divulgamos nossas aulas ao vivo e falamos sobre os concursos abertos, expectativas de novos concursos, revisões de véspera, e por aí vai...

http://t.me/estrategia_ti



Criamos um perfil no Instagram ... e qual o objetivo? Fazer com que os alunos percam tempo nas redes sociais? Claro que não!! Estamos consolidando diversos posts dos professores! São dicas especiais, um patrimônio que deve ser explorado por todos os concurseiros de TI!

http://instagram.com/estrategiaconcursosti

CRONOGRAMA DE AULAS

Vejamos a distribuição das aulas:

AULAS	TÓPICOS ABORDADOS	DATA
Aula 00	Crimes eletrônicos. Engenharia social. Phishing. Pharming. Sniffer. Negação de serviço (DoS e DDos). Softwares maliciosos (malwares).	06/12/19
Aula 01	Endereçamento IP. Serviço de resolução de nomes (DNS). Tradução de endereços de rede (NAT). Provedor de acesso à Internet (ISP). Rastreamento de e-mail. Busca pelo responsável de um endereço IP. Coleta de informações com validade jurídica.	08/12/19
Aula 02	Busca e apreensão. Solicitação de perícia. Conceitos de computação forense. Ordem de volatilidade. MAC Times. Análise da linha do tempo. Cadeia de custódia. Etapas da computação forense. Normas técnicas. Procedimento operacional padrão.	08/12/19
Aula 03	Post mortem forensics. Proteção da mídia. Duplicação forense. Verificação de integridade. Exame dos dados. Análise das informações.	08/01/20
Aula 04	Live forensics. Captura de informações. Duplicação forense. Verificação de integridade. Exame dos dados. Análise das informações.	10/01/20
Aula 05	Sistemas de arquivos. Representação de dados. Mídias de armazenamento: (a) discos rígidos; (b) memórias flash; (c) discos ópticos. Particionamento. FAT. NTFS. EXT2, EXT3, EXT4. Outros.	15/01/20
Aula 06	Recuperação de dados. Tipos de carving. Carving baseado em: (a) cabeçalho/rodapé ou cabeçalho/tamanho máximo; (b) estrutura do arquivo; (c) blocos de conteúdo; (d) sistema de arquivos.	30/01/20
Aula 07	Quebra de senhas. Detecção de conteúdo criptografado. Recuperação de senhas: (a) recuperação direta; (b) ataque do dicionário; (c) ataque de força bruta; (d) pré-computado (rainbow tables); (e) híbrido.	08/02/20
Aula 08	Análise de sistemas Windows. Registro. Eventos. Lixeira. Prefetch. Outras fontes de análise.	03/03/20
Aula 09	Análise em dispositivos móveis. Tecnologia GSM. Cartões SIM. Memória interna. Preservação da evidência. Conexão com o dispositivo. Coleta dos dados: (a) coleta automática; (b) coleta direta; (c) coleta manual; (d) coleta avançada. Análise das informações.	07/03/20
Aula 10	Network forensics. Protocolos e equipamentos de redes. Fontes de vestígios cibernéticos. Captura e análise de tráfego. Criptografia aplicada aos protocolos.	10/03/20
Aula 11	Análise de malwares. Técnicas estáticas e dinâmicas. Uso de máquinas virtuais. Análise de malwares para Windows. Comportamento do malware. Técnicas contra a engenharia reversa.	16/03/20
Aula 12	Análise de pornografia infantojuvenil: Pedofilia. A legislação. Caracterização do crime. Detecção de conteúdo e de compartilhamento de arquivos. Laudo pericial: Características. Itens de um laudo: (a) introdução; (b) resumo do incidente; (c) objetivo; (d) metodologia; (e)	20/03/20

	resultado; (f) conclusão/resposta aos quesitos; (g) considerações finais; (h) anexo(s).	
Aula 13	Antiforense digital. Proteção: criptografia. Destruição: (a) física; (b) lógica. Ocultação: (a) ADS (Alternate Data Stream); (b) partições ocultas; (c) slackering; (d) esteganografia. Ofuscação. Falsificação. Prevenção à análise. Subversão de ferramentas.	24/03/20

Essa é a distribuição dos assuntos ao longo do curso. Eventuais ajustes poderão ocorrer, especialmente por questões didáticas. De todo modo, sempre que houver alterações no cronograma acima, vocês serão previamente informados, justificando-se.

INTRODUÇÃO AO ESTUDO DA COMPUTAÇÃO FORENSE

1 - Considerações Iniciais

Na aula de hoje vamos estudar assuntos que antecedem a computação forense, ou seja, os crimes eletrônicos, alguns tipos de ataques e malwares (softwares maliciosos). Boa aula!

2 - Crimes Eletrônicos

2.1 – Conceitos

Apesar do curso ser voltado à computação forense, temos que saber o que vem antes dela, ou seja, o porquê da existência da coleta e análise de vestígios para a geração da evidência! Confuso? Calme, aos poucos vamos desmistificando essa fascinante área! Além disso, crimes eletrônicos também são cobrados em provas de concurso!

Você já deve ter ouvido que vivemos na era da informação, ou seja, na atualidade a informação pode valer muito mais do que a produção de bens materiais. Um exemplo disso foi a venda do Whatsapp para o Facebook, por mais de 20 bilhões de dólares, em 2014! Obviamente, esse valor não foi associado apenas aos servidores, equipamentos e outros bens, além de imóveis. O que estava em jogo era a quantidade de usuários do serviço, mais de 600 milhões na época.

Diante disso, a criminalidade também tem migrado do mundo real para o virtual. Você já deve ter lido ou ouvido muito a respeito de furto de dados, invasões de sistemas, alteração de dados de forma fraudulenta, entre outros. Mudanças na legislação também foram necessárias, para que criminosos não ficassem impunes. Tudo isso e mais um pouco estudaremos a partir de agora.

Primeiro, vamos aos nomes dados ao crime eletrônico: crimes cibernéticos, crimes virtuais, *cybercrimes*, crimes digitais, e-crimes, crimes informáticos, entre outros. Todos possuem o mesmo objetivo: utilizar a tecnologia como meio ou fim para cometer ilícitos. Como é algo relativamente novo, não há na doutrina uma definição pacificada sobre crime eletrônico. A seguir são mostradas algumas definições encontradas na literatura:

a) Crime no qual foi utilizada tecnologia para facilitar a atividade criminosa;

b) Não são, necessariamente, novos crimes, pois podem ser crimes clássicos que exploram o poder proporcionado pela tecnologia bem como o uso de redes de computadores, em especial, a Internet.

De acordo com Huebner et al. (2003), com a intenção de criar uma definição didática, os crimes eletrônicos foram enumerados e classificados por áreas, conforme mostrado a seguir:

a) Crimes centrados no computador: a atividade criminosa tem como objetivo sistemas computacionais, redes de computadores, mídias de armazenamento ou outros dispositivos computacionais. Ex.: perturbação do funcionamento de um sítio de comércio eletrônico;

b) Crimes auxiliados por computador: computadores são utilizados como ferramentas para o auxílio de atividades criminosas, sendo que a utilização de computadores não é estritamente necessária. Ex.: divulgação de material que afeta a reputação de alguém;

c) Crimes por computador incidentais: a utilização de computadores é eventual. Ex.: contabilidade informatizada utilizada para manter os registros de propinas pagas a políticos corruptos (poderia ser utilizado papel e caneta, mas optou-se em utilizar uma planilha eletrônica).

A classificação que tem encontrado mais adeptos é a que divide os crimes eletrônicos em próprios (exclusivamente cibernéticos) e impróprios (abertos), conforme mostrado a seguir.

a) Crime eletrônico próprio: é aquele que exige e depende necessariamente da utilização de ambiente computacional. Ou seja, se não existisse a tecnologia, não existiria o crime! Alguns exemplos clássicos são a criação e disseminação de códigos maliciosos (malwares), ataques de negação de serviço, a invasão e destruição de banco de dados, entre tantos outros. No Brasil, a Lei 12.737/2012, conhecida como “Lei Carolina Dieckmann”, trata de alguns crimes eletrônicos próprios (e é cobrada em provas de concurso!);

b) Crime eletrônico impróprio: é aquele em que o ambiente computacional é utilizado como meio para a execução da conduta ilícita. Ou seja, o crime já existia ou pode vir a existir, e o uso do ambiente computacional é opcional. Alguns exemplos são os crimes contra a honra, ameaça, falsificação, estelionato, furto, entre outros.

Bom, já vimos algumas classificações do crime eletrônico, agora vamos analisar a materialidade e a autoria, pois não basta haver um boato que um crime ocorreu, deve-se comprovar que de fato ocorreu e deve-se buscar o responsável pelo mesmo. Aí entra a polícia judiciária (Polícia Civil ou Federal) e, em muitos casos, será solicitada uma perícia técnica (computação forense) para o órgão de perícia criminal competente.



Embora o assunto abordado nesta aula e nas seguintes faça menção a crimes, muitos conceitos podem ser adotados em perícias cíveis ou atividades em órgãos que não atue em perícia criminal. Ex.: órgãos de auditoria, agências ou setores de inteligência, área de suporte etc.

O sistema processual brasileiro é fundado sobre o princípio da **livre convicção motivada e fundamentada do juiz**. Para efetuar o convencimento do juiz, as partes envolvidas têm a oportunidade de produzir **provas**, sendo a prova tudo aquilo que seja útil no convencimento do julgador, **na busca da verdade**. Não preciso dizer que a prova pericial é considerada a mais importante no caso de um crime eletrônico, certo? Não é à toa que a perícia é conhecida como a rainha das provas 😊, tendo um "peso" maior do que documentos e testemunhas (claro que na prática, o juiz pode decidir conforme seu convencimento, sempre de forma motivada e fundamentada).

A prova pericial pode ser solicitada por qualquer das partes ou de ofício pelo magistrado. Diante da **volatilidade** do ambiente computacional (os dados "somem", ou as pessoas apagam 😊), **nem sempre é possível a realização de perícia no dispositivo**, sendo também utilizada a prova documental através de atas notariais (veremos esse assunto em breve), documentando: capturas de telas, mensagens em telefones celular, publicações em redes sociais, entre outros.

Como já mencionado anteriormente, a Lei "Carolina Dieckmann" (Lei 12.737/12) é um exemplo que contempla crimes eletrônicos próprios, e vem sendo cobrada em provas de concurso, especialmente para perito. Vamos dar uma olhada a seguir, mas eu **recomendo que você também leia a letra fria da lei**.

A Lei 12.737/12 dispõe sobre a **tipificação criminal de delitos informáticos**, altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal – C.P.) e dá outras providências. Basicamente foram acrescidos no C.P. os artigos 154-A e 154-B, e os artigos 266 e 298 obtiveram nova redação. Ou seja, você pode ler esses artigos diretamente no código penal, sem ler a lei "Carolina Dieckmann".

A seguir transcrevo e comento principalmente os artigos e parágrafos referentes a questões técnicas, com pouca ou nenhuma atenção dada aos artigos, parágrafos ou incisos referentes às penas. Por isso, novamente, **sugiro a leitura da letra fria da lei**!

Invasão de Dispositivo Informático

> *Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.*

Vamos analisar cada item desse artigo:

a) **Dispositivo informático**: pode ser considerado qualquer dispositivo eletrônico que processe, transmita e/ou armazene informações digitais (ex.: *smartphones*, computadores, *smart* TVs, *tablets*, entre outros);

b) **Conectado ou não à rede de computadores**: o dispositivo pode ter ou não conexão a uma rede (local ou a Internet). No caso de não haver conexão com qualquer rede, a invasão possível é o acesso físico ao equipamento;

c) **Mediante violação indevida de mecanismo de segurança**: Um mecanismo de segurança pode ser um software instalado (*antimalware*, *firewall*, etc.), um mecanismo do próprio sistema operacional (exigência de senha para *logon* do usuário), mecanismo de segurança física (catracas, dispositivo de

leitura biométrica, etc.) Ou ainda, se alguém instala um *backdoor* ou algum outro tipo de *malware* sem o consentimento do proprietário do dispositivo, há uma violação da segurança ou facilitação do acesso indevido;

d) **Com o fim de obter, adulterar ou destruir dados ou informações**: O simples fato de ler dados/informações já garante a obtenção dos mesmos (o difícil seria provar), mesmo sem ter realizado uma cópia. Adulterar geralmente decorre de uma modificação intencional, mas pode ocorrer de forma acidental (queda de energia, por exemplo). Destruir dados/informações pode decorrer da exclusão (que podem ser recuperados, dependendo da situação) ou através de aplicação de *wipe* (técnica antiforense a ser mostrada nesse curso);

e) **Sem autorização expressa ou tácita do titular do dispositivo**: Garante que se houver a autorização, como por exemplo a autorização dada a um *pentester* (profissional pago para testar vulnerabilidades em redes e sistemas), o ato será considerado lícito;

f) **Ou instalar vulnerabilidades para obter vantagem ilícita**: uma possível interpretação é a instalação de *malwares* ou de dispositivos físicos (ex.: *Keylogger* físico, colocado entra o gabinete de computador e o teclado) para facilitar a invasão.

Malwares e afins

> *§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.*

O § 1º está relacionado a quem desenvolve um *malware*, oferece, vende ou o difunde. Ou ainda, algum dispositivo físico que permita a invasão de dispositivo informático alheio para os fins definidos no *caput*. Obviamente, se um *pentester* desenvolver um *malware* apenas para realizar uma invasão com o consentimento do proprietário do dispositivo, essa conduta seria considerada lícita, conforme já vimos.

> *§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido.*

No § 3º, além de mencionar a obtenção de conteúdo privado (ex.: diálogos armazenados em um servidor de rede social) e informações sensíveis (ex.: informações guardadas em um servidor de armazenamento na nuvem), aborda um novo elemento: o controle remoto não autorizado. Há situações em que uma invasão ocorre, permitindo a visualização de conteúdo, mas não necessariamente possibilita o controle remoto. Tal controle poderia ser realizado pelo atacante, caso o mesmo obtenha privilégio de *root* (Linux) ou Administrador (Windows).

Interrupção ou Perturbação de Serviço Telegráfico, Telefônico, Informático, Telemático ou de Informação de Utilidade Pública

O Art. 266 do Código Penal possuía parágrafo único antes da criação da Lei 12.737/12. Após a criação da lei, o parágrafo único foi transformado em § 2º e o § 1º foi inserido. Para um melhor entendimento, o Art. 266 será transcrito na íntegra e apenas o § 1º será comentado.

Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena - detenção, de um a três anos, e multa.

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime for cometido por ocasião de calamidade pública.

Podemos ver que se trata do ataque de **negação de serviço (DoS – *Deny of Service***, assunto que veremos ainda nesta aula!) direcionado a dispositivos informáticos, que, até então, não era crime! A punição também está prevista caso o serviço já esteja inoperante e alguém aplique um ataque de DoS para dificultar ou até mesmo impedir o reestabelecimento do mesmo.

Falsificação de Cartão

Ao Art. 298 do C.P. foi adicionado o parágrafo único. Para um melhor entendimento, o Art. 298 será transcrito na íntegra e apenas o parágrafo único será comentado.

Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:

Pena - reclusão, de um a cinco anos, e multa.

- ***Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.***

Antes da Lei 12.737/12, a clonagem de cartões de crédito ou débito não era crime, pois não estava explícito que cartões de crédito ou débito se equiparavam a documentos particulares.

2.2 – Questões Comentadas

1. **(FUNDATEC/IGP-RS - 2017) A Lei nº 12.737/2012, também conhecida como Lei dos Crimes Cibernéticos, dispõe sobre a tipificação criminal de delitos informáticos. O artigo 154-A dessa lei diz: "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa". A redação desse artigo mostra a intenção do legislador de tutelar valores protegidos constitucionalmente. Qual o bem jurídico protegido pelo artigo 154-A da Lei de Crimes Cibernéticos?**

A) Segurança dos dados.

B) Dispositivos informáticos.

C) Rede de computadores.

D) Privacidade.

E) Livre acesso à informação.

Comentários:

Embora a questão tenha sido cobrada na parte específica da prova de perito criminal - área: computação forense, parece mais uma questão de direito constitucional, não é mesmo?

Pois é...das alternativas apresentadas, qual delas remete à Constituição? O art. 5, X fala o seguinte: "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;". Mas, mesmo que você não tivesse esse conhecimento, bastaria pensar...será que segurança dos dados, dispositivos informáticos, rede de computadores e livre acesso à informação seriam bens jurídicos? Como o crime é a invasão de um dispositivo informático com o fim de obter, alterar ou destruir dados, o mais lógico seria a proteção da privacidade da vítima. Portanto, a **alternativa D** está correta e é o gabarito da questão.

2. (IBFC/Polícia Científica do Paraná - 2017) Assinale a alternativa correta, considerando o disposto expressamente na Lei nº 12.737, de 30/11/2012 (Lei dos crimes cibernéticos), sobre a pena aplicável a quem invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita?

A) Detenção de 1 (um) a 2 (dois) anos, e multa, aumentando-se a pena de um terço à metade se da invasão resultar prejuízo moral.

B) Detenção de 1 (um) a 2 (dois) anos, e multa, aumentando-se a pena de um sexto a um terço se da invasão resultar prejuízo econômico.

C) Detenção de 3 (três) meses a 1 (um) ano, e multa, aumentando-se a pena de um sexto a um terço se da invasão resultar prejuízo econômico.

D) Detenção de 3 (três) meses a 1 (um) ano, e multa, aumentando-se a pena de um terço à metade se da invasão resulta prejuízo moral.

E) Detenção de 6 (seis) meses a 2 (dois) anos, e multa, aumentando-se a pena de um sexto a um terço se da invasão resulta prejuízo moral.

Comentários:

Sacanagem cobrar a pena e, ainda, o aumento de pena! Mas é assim mesmo, tem banca que cobra o detalhe do que está escrito na lei para evitar recurso! Como eu disse antes, é bom dar uma lida na "letra fria" da lei 12.737/12. Vejamos:

Art. 154-A. Invadir dispositivo [...]

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

[...]

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

[...]

Portanto, a **alternativa C** está correta e é o gabarito da questão.

3. (IBFC/Polícia Científica do Paraná - 2017) Assinale a alternativa correta, considerando o disposto expressamente na Lei no 12.737, de 30/11/2012 (Lei dos crimes cibernéticos), sobre a AÇÃO PENAL nos casos do crime praticado por quem invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter informações sem autorização expressa ou tácita do titular do dispositivo:

A) Nesses casos, somente se procede mediante representação, mesmo que o crime seja cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos

B) Nesses casos, procede-se independentemente de representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios.

C) Nesses casos, procede-se independentemente de representação, salvo se o crime é cometido contra empresas concessionárias de serviços públicos.

D) Nesses casos, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

E) Nesses casos, a ação penal é sempre pública e incondicionada.

Comentários:

Essa questão é mais tranquila que a anterior. Mesmo que você não lembre exatamente o que está escrito na lei, pense na seguinte lógica: existem diversas invasões todos os dias, sendo que muitas vezes a vítima nem "dá bola", formata o HD e continua utilizando, sem registrar B.O. Então não seria razoável buscar o responsável se a vítima não está nem aí para o crime...

Por outro lado, quando é contra a Administração Pública, a coisa é mais embaixo! Seria lógico buscar o responsável, mesmo sem representação. Correto?

Vejamos o que diz a lei: "Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer

dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.”. Logo, a **alternativa D** está correta e é o gabarito da questão.

4. (UFMT/IF-MT - 2015) Sobre a tipificação dos delitos informáticos segundo a Lei nº 12.737/2012, assinale a afirmativa correta:

A) Pratica crime de invasão de dispositivo informático aquele que, com autorização expressa do titular do dispositivo, instala vulnerabilidades para obter vantagem ilícita.

B) Pratica o crime de perturbação de serviço telemático, telefônico ou informático aquele que interrompe o serviço telemático, telefônico ou informático, salvo se cometido por ocasião de calamidade pública.

C) Pratica crime de invasão de dispositivo informático aquele que adultera ou destrói dados ou informações sem autorização expressa ou tácita do titular do dispositivo.

D) Pratica o crime de falsificação de documento público aquele que falsifica, no todo ou em parte, cartão de crédito ou de débito, obtendo ou não vantagem ilícita.

Comentários:

(A) Se fosse crime, um pentester seria criminoso, mesmo com a autorização do seu cliente! (B) Não tem sentido deixar de ser crime, justamente por ocasião de calamidade pública, quando mais se precisa de serviços de telefonia e de informática! **(C) Perfeito! Não basta invadir, tem que haver “o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”;** (D) É realizada uma equiparação a documento particular, e não documento público!

5. (SIGMA/Câmara Municipal de Carapicuíba-SP - 2013) Cinco meses após hackers roubarem e divulgarem na internet fotos íntimas da atriz Carolina Dieckmann, o Congresso Nacional aprovou proposta que tipifica crimes cibernéticos. Batizada de “Lei Carolina Dieckmann”, a legislação que torna crime a invasão de computadores foi sancionada por Dilma Rousseff em dezembro de 2012. Essa lei é a Lei Nº:

A) 12.373.

B) 12.737.

C) 10.737.

D) 10.373.

Comentários:

Trata-se da Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Portanto, a **alternativa B** está correta e é o gabarito da questão.

3 - Engenharia Social

3.1 – Conceitos

Embora conceitualmente haja diferença entre a nomenclatura: hacker (quem possui muito conhecimento e o utiliza para o "bem") e cracker (quem possui muito conhecimento e o utiliza para obter vantagens, cometer crimes, etc.), muitas vezes hacker é utilizado como sinônimo de cracker, principalmente pela mídia, e muitas vezes pela banca! Fique atento!

Engenharia social é um termo frequentemente utilizado na comunidade de segurança, mas nem tanto na comunidade de T.I. em geral! Trata-se da "arte de enganar", como diria Kevin Mitnick, um famoso hacker que já foi cracker um dia! O título do livro escrito por ele e por William Simon diz tudo: "A Arte de Enganar – Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação". Notem que no livro foi utilizado o termo hacker!

Na engenharia social são utilizadas técnicas de persuasão para convencer pessoas a fornecerem informações, geralmente sensíveis, como senhas, dados de cartões de crédito, dados relativos a documentos, entre outros. Antigamente, o meio mais utilizado para obtenção de tais informações era o telefone, mas atualmente o meio mais utilizado é o envio de e-mails, o que permite atingir um número maior de vítimas a um custo bem mais baixo.

Muitos criminosos utilizam as técnicas de engenharia social antes de tentarem a invasão de sistemas, pois é muito mais fácil enganar pessoas do que possuir conhecimentos avançados ou contar com a sorte de sistemas alvo não estarem devidamente atualizados. É muito mais fácil ser bom de papo do que dominar assuntos relacionados à sistemas operacionais, redes, programação etc. 😊

3.2 – Questões Comentadas

6. (FUNDATEC/PGE-RS – 2010) Essa questão baseia-se na palestra intitulada "A Arte de Enganar", ministrada pelo ex-hacker e atual consultor de segurança Kevin Mitnick, durante o Campus Party 2010, que ocorreu em São Paulo, em janeiro desse ano. Nessa palestra, Mitnick abordou métodos usados por hackers para obter informações sigilosas. Segundo ele "Muitos ataques de hackers não necessitam de grande conhecimento técnico, mas sim de poder de convencimento para que a própria vítima forneça as informações desejadas". Mitnick admitiu que, muitas vezes, se valeu de truques de convencimento verbal e mentiras que o levaram a invadir diversos sistemas nos quinze anos em que se manteve nesta atividade. Na opinião de Mitnick, bastava persuadir funcionários mais desavisados a compartilharem informações vitais, como nomes de login e senhas; foi assim que ele afirma ter invadido a rede da empresa Sprint, se passando por um engenheiro da firma Nortel Networks para o qual os funcionários passaram dezenas de logins e senhas para o acesso aos switches. Nesse caso, a utilização da persuasão, dissimulação e mentiras verbais para convencer funcionários a compartilharem informações vitais, como nomes de login e senhas, para ter acesso não autorizado a diversos ativos de redes, como, por exemplo, switches, caracteriza-se por ser um método de ataque denominado

A) Hoax.

B) Spyware.

C) Adware.

D) Keyloggers.

E) Engenharia Social.

Comentários:

(a) O tamanho do enunciado assusta, mas a questão é bem tranquila! Hoax é sinônimo de boato, aquelas correntes que falam que tal coisa vai acontecer, para passar para 50 amigos, etc., só serve para encher as caixas de e-mail, gerar tráfego inútil na rede, entre outras coisas; (b) Spyware, (c) adware e (d) keyloggers são malwares que veremos adiante. **(e) Algumas palavras-chave que eu destaco para definir a resposta como engenharia social: convencimento verbal, mentiras, persuasão. Além de tudo, Kevin Mitnick era o mestre na arte de enganar! Até escreveu um livro sobre isso, como já vimos!**

7. (CESPE/Polícia Federal – 2013) O ser humano possui traços psicológicos e comportamentais que o tornam vulneráveis a ataques de engenharia social, como a vontade de ser útil, a busca por novas amizades, esteganografia e autoconfiança.

Comentários:

Engenharia social está relacionada à psicologia, pois lida diretamente com o comportamento do ser humano. Os exemplos dados estavam indo muito bem...com exceção de esteganografia! Esteganografia é uma técnica utilizada para esconder dados e será abordada na aula sobre antiforense digital, neste curso. Portanto, a **afirmativa está errada.**

8. (IBFC/PC-RJ – 2013) Existe um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. Estamos falando do método de:

A) Colarinho Branco.

B) Engenharia de Serviço.

C) Criptografia Privada.

D) Engenharia Social

E) Sociologia criptográfica.

Comentários:

(a) Crime de colarinho branco é cometido por alguém respeitável (ou deveria ser); (b) Engenharia de serviço? (c) Criptografia privada e (e) sociologia criptográfica foram falta de criatividade do examinador mesmo 😊 Ficou fácil essa, heim? Logo, a **alternativa D** está correta e é o gabarito da questão. Detalhe: prova para perito criminal!

9. (UESPI/PC-PI – 2014) A utilização de práticas para obter acesso a informações sigilosas em organizações e sistemas computacionais, por meio da exploração de confiança das pessoas com habilidades de persuasão, é chamada de

A) engenharia reversa.

B) spyware.

C) engenharia social.

D) worm.

E) botnet.

Comentários:

(a) Engenharia reversa é "voltar uma ou mais etapas", se você tem um programa executável e não possui mais o programa fonte, pode tentar aplicar a engenharia reversa, tentando descompilá-lo, por exemplo; (b) spyware, (d) worm e (e) botnet são malwares que veremos mais adiante. Note que mais uma vez foi utilizada a palavra-chave persuasão para definir engenharia social! Fique atento! Logo, a **alternativa C** está correta e é o gabarito da questão.

10. (INSTITUTO CIDADES/CONFERE – 2016) São objetivos da engenharia social, EXCETO

A) Técnica para prevenir ataques aos ativos.

B) Espionagem industrial.

C) Obter informações privilegiadas para ter vantagem.

D) Roubo de senhas de bancos ou cartões de crédito.

Comentários:

(a) A engenharia social é uma técnica de persuasão, é considerada um tipo de ataque e não é uma forma de prevenção de ataque! (b) é possível a espionagem industrial através de mensagens de engenharia social, depende se a vítima é persuadida; (c) se a vítima fornecer informações, com certeza um objetivo da engenharia social foi atingido! (d) na verdade, não é bem um roubo, mas sim a persuasão aplicada a uma vítima e ela pode executar atividades, como a instalação de algum malware que colete e envie senhas e outros dados sensíveis ao criminoso...enfim, não estaria totalmente correta, mas ainda sim estaria menos errada que a alternativa A. Logo, a **alternativa A** é o gabarito da questão.

11. (FCC/TRT-24ª Região – 2017) Um Técnico de Informática, ao acessar o site da organização para a qual trabalha, encontrou-o totalmente desfigurado, com o conteúdo das páginas alterado. Ao buscar razões para este tipo de ataque que viola a segurança das informações, verificou que um atacante, para desfigurar uma página web, pode:

– explorar erros da aplicação web;

– explorar vulnerabilidades do servidor de aplicação web;

– explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação web;

– invadir o servidor onde a aplicação web está hospedada e alterar diretamente os arquivos que compõem o site;

– furtar senhas de acesso à interface web usada para administração remota.

O Técnico concluiu, corretamente, que este tipo de ataque é conhecido como

A) inundação UDP.

B) engenharia social.

C) wardriving

D) IP spoofing.

E) Defacement

Comentários:

Para todo esse enunciado, preste atenção no que foi realizado: uma página Web foi desfigurada. Se você marcou engenharia social, foi induzido ao erro...coloquei essa questão de propósito para ver se você estava atento, pois a questão não fala em persuasão ou algo similar 😊 (a) inundação UDP seria algo relacionado à flood; (b) engenharia social é a arte de enganar! (c) wardriving é a prática de procurar por redes sem fio dirigindo um automóvel; (d) IP spoofing é a falsificação de endereçamento IP. **(e) Defacement é a pichação, desfiguração de páginas Web**, um tipo de ataque que o grupo Anonymous gosta bastante. Mesmo não estando no escopo do curso, acabamos de aprender mais um assunto!

12. (FUNDATEC/IGP-RS – 2017) O conceito de Segurança da Informação (SI) pode ser definido simplesmente como o conjunto de medidas que possuem o objetivo de tornar as informações seguras, sendo a cultura dos usuários um dos alicerces da segurança da informação mais sensíveis. Qual é a técnica utilizada pelos criminosos que explora diretamente a cultura dos usuários?

A) Esteganografia.

B) Criptografia.

C) Autenticidade.

D) Confidencialidade.

E) Engenharia social.

Comentários:

Mais uma palavra-chave interessante: cultura. Quando se fala em segurança da informação, temos mecanismos (hardware, software), políticas (normas, regras) e cultura (conhecimento dos usuários). Esteganografia e criptografia são mecanismos de segurança relacionados à propriedade de confidencialidade. Autenticidade é uma propriedade que, por exemplo, pode ser aplicada com a assinatura digital. E a engenharia social é uma forma de explorar a cultura dos usuários. Por isso é importante investir em palestras e treinamentos aos funcionários, para que não sejam vítimas da engenharia social, entre outros tipos de ataque ou golpe. Logo, a **alternativa E** está correta e é o gabarito da questão.

13. (IESES/IGP-SC – 2017) Considerando as práticas do que se denomina 'Engenharia Social' no contexto da Segurança da Informação, é correto afirmar que:

A) Um 'ataque' de engenharia social pode utilizar estratégias de relacionamento pessoal para obtenção de informações sigilosas.

B) A utilização de certificados digitais A3 é mais adequada que certificados A1.

C) Algoritmos de 'força bruta' são um instrumento comumente utilizados para descoberta de informações.

D) A instalação de softwares detectores de 'phishing' é uma estratégia para evitar ataques de um engenheiro social.

Comentários:

(a) É isso mesmo! Pode ser aplicada com conhecidos ou desconhecidos! (b) Assinatura digital não tem nada a ver com o assunto! (c) Força bruta é uma das formas de descobrir uma senha ou chave criptográfica, por exemplo (veremos na aula sobre quebra de senhas, neste curso); (d) Como seria um software detector de phishing? Quando existem golpes já conhecidos, pode-se utilizar algum filtro por palavras-chave, títulos de e-mails, etc., mas nada muito além disso!

4 - Phishing

4.1 – Conceitos

Existem outros termos para o mesmo propósito da engenharia social, como é o caso de *phishing* (mesma ideia de *fishing* - pescaria), ou *phishing scam* (golpe). Este último geralmente é associado a golpes financeiros. Imagine o seguinte cenário: um e-mail é enviado com um formulário a várias pessoas (uma lista contendo milhões de endereços de e-mail), alegando ser de um banco e que é necessária uma atualização dos dados,

entre eles a senha. No momento em que alguém preenche o formulário e o envia, o criminoso pode utilizar estes dados para realizar movimentações financeiras.

Pelos motivos expostos, os sítios de bancos e comércio eletrônico em geral, investem pesado em mecanismos de proteção que tentam diminuir as vítimas de engenharia social e phishing. Por exemplo, a maioria dos bancos exige que o usuário utilize um cartão com chip, um *token* ou alguma outra forma de dificultar a vida dos criminosos. Assim, mesmo que alguns dados sensíveis sejam coletados, podem ser inúteis ao propósito do criminoso.

Um termo que também é cobrado em provas de concurso é ***spear phishing***, que possui o diferencial de ser enviado a um **grupo específico como alvo**. Então, em vez de enviar a uma lista de e-mails qualquer, são selecionados endereços de uma determinada organização, associação, gerência, enfim, um grupo de pessoas que possuem algum tipo de afinidade. Assim, o conteúdo utilizado para "fisgar" a vítima é mais específico, o que pode tornar o ataque mais exitoso.

4.2 – Questões Comentadas

14. (FCC/TRT-9ª Região – 2013) É um tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social, ocorre por meio do envio de mensagens eletrônicas que

- tentam se passar pela comunicação oficial de uma instituição conhecida, tal como banco, empresa ou site popular;

- procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;

- informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;

- tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas web.

Este meio de ataque é conhecido como

A) trojan.

B) phishing.

C) malware.

D) sniffing.

E) spoofing.

Comentários:

Enunciado extenso, mas questão tranquila, né? "Isca", persuasão, induzimento para fazer algo...phishing! Um novo termo surgiu: sniffing é a coleta de pacotes na rede (veremos ainda nesta aula). Logo, a **alternativa B** está correta e é o gabarito da questão.

15. (FGV/SUDENE-PE – 2013) Um usuário acessa sua caixa de mensagens e abre uma mensagem supostamente enviada pelo seu banco solicitando que ele acesse o site do banco e atualize alguns dados. O usuário clica no link e um site idêntico ao do banco aparece. Ele entra com a sua senha, atualiza os dados e os transmite. Depois de algum tempo, ele percebe que foi enganado, pois uma grande quantia foi retirada da sua conta. Assinale a alternativa que indica o tipo de ataque que ele sofreu.

A) DDoS.

B) phreaking.

C) DoS.

D) phishing.

E) adware.

Comentários:

A clássica "isca" que foi fisgada! Está claro que a resposta é phishing. E as outras, por que estão erradas? DoS e DDoS são ataques de negação de serviço. Phreaking é a atividade de cracking aplicado à telefonia. Adware é um malware que mostra propagandas (veremos adiante). Logo, a **alternativa D** está correta e é o gabarito da questão.

16. (FGV/DPE-RO – 2015) Para tentar diminuir as possibilidades do ataque phishing deve-se:

A) realizar a leitura de e-mail através de sites web, pois o e-mail não é trazido para a máquina do cliente;

B) configurar adequadamente um filtro para pacotes ICMP no servidor de correio;

C) usar o serviço NFS no cliente de e-mail;

D) implantar filtros para mensagens spam ou em "black-list";

E) realizar leitura de e-mail através do protocolo pop ou imap com ssl, usando criptografia na rede.

Comentários:

O ataque de phishing tem como objetivo enganar o ser humano, então as alternativas que falam um utilizar um determinado protocolo, sistema de arquivos (NFS) ou plataforma não ajudam a preveni-lo. O que pode

ajudar é um filtro de mensagens de spam ou uma lista negra. Claro que se for um phishing direcionado a poucos alvos e tal mensagem ou remetente não estiver em uma lista negra, a mensagem acabaria chegando na caixa de mensagens e o usuário deveria ter conhecimento para não cair na "isca". Logo, a **alternativa D** está correta e é o gabarito da questão.

17. (FCC/ELETROBRAS-ELETROSUL - 2016) Considere, por hipótese, que a Eletrosul deseja aumentar a segurança das informações utilizando registros das atividades de seus colaboradores. A partir da análise destes registros armazenados em arquivo ou em base de dados, a empresa pode ser capaz de:

- detectar o uso indevido de computadores, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema;

- detectar um ataque, como de força bruta, ou a exploração de alguma vulnerabilidade;

- rastrear ou auditar as ações executadas por um usuário no seu computador, como programas utilizados, comandos executados e tempo de uso do sistema;

- detectar problemas de hardware ou nos programas e serviços instalados no computador.

Estes registros são denominados

A) backups.

B) phishing.

C) logs.

D) hashes.

E) firewalls.

Comentários:

Registros de atividades ocorridas (conhecidos como logs) são ótimos para uma auditoria ou perícia! E as demais alternativas? Backup é uma cópia de segurança. Phishing é aquela velha "isca". Hashes são códigos gerados a partir de algoritmos, tendo como principal finalidade a garantia de integridade (veremos em detalhes, em aula futura). Firewalls são filtros de pacotes de rede! Logo, a **alternativa C** está correta e é o gabarito da questão.

18. (CESPE/TCE-PA – 2016) Diferentemente dos golpes de phishing, os ataques de spear phishing são realizados mediante o envio aleatório e em massa de emails enganosos para múltiplos usuários, para a obtenção de informações bancárias das vítimas ou apropriação da identidade delas.

Comentários:

A CESPE inverteu os conceitos. Spear phishing é a aplicação de phishing focado em um grupo específico. Logo, a questão está **errada**.

19. (FCC/Prefeitura de Teresina-PI – 2016) O usuário de um computador instalado na rede local de computadores - LAN gerenciada pelo Analista de Suporte informou e questionou sobre o recebimento de uma mensagem de e-mail que solicitava a atualização das suas informações de usuário na LAN. Identificando que se tratava de uma mensagem falsa, o Analista concluiu que se tratava de um ataque do tipo.

A) DoS.

B) Spoofing.

C) Flooding.

D) Spam.

E) Phishing.

Comentários:

Mais uma questão que deixa claro o recebimento de uma "isca" por e-mail, ou seja, phishing! E as outras alternativas? DoS é negação de serviço. Spoofing é a falsificação, por exemplo, de um endereço. Flooding é a inundação de mensagens. Spam é o envio de mensagens indesejadas. Logo, a **alternativa E** está correta e é o gabarito da questão.

20. (COSEAC/Prefeitura de Maricá-RJ – 2018) Na segurança da Informação existe um tipo de ataque em que iscas como "mensagens não solicitadas" são utilizadas para capturar senhas e dados de usuários na Internet. Esse ataque é conhecido como:

A) spoofing.

B) hijacking.

C) engenharia social.

D) phishing.

E) cookies.

Comentários:

(a) Spoofing é a falsificação, que pode ser de um endereço de e-mail do remetente, o endereço IP, etc.; (b) Hijacking é um termo utilizado para sequestro, como por exemplo o sequestro de sessão; (c) Engenharia social é a "arte de enganar", não necessariamente através de "iscas"; **(d) O próprio nome phishing indica a pescaria (fishing), ou seja, através de uma "isca" procura-se "pescar" informações da vítima;** (e) Cookies são utilizados para armazenar dados de navegação para "lembrar" posteriormente o que o usuário fez ou por onde navegou. Ex.: quais produtos o usuário viu em um sítio de comércio eletrônico.

21. (FGV/AL-RO – 2018) O tipo de ataque na Internet em que pessoas comuns são contatadas por e-mail, com mensagens que parecem genuínas, contendo nomes e informações que fazem referência a empresas conhecidas, como bancos, porém, contendo links disfarçados para arquivos maliciosos, é denominado

A) Spoofing.

B) DoS.

C) DDoS.

D) Phishing.

E) Bluebugging.

Comentários:

(a) Spoofing é a falsificação, que pode ser de um endereço de e-mail do remetente, o endereço IP, etc.; (b) Dos (Deny of Service) é o ataque de negação de serviço, cujo objetivo é inutilizar ou dificultar o uso de um determinado serviço; (c) DDoS é o mesmo que DoS, porém de forma distribuída; **(d) No caso da questão, o link seria a "isca" para o ataque de phishing;** (e) Bluebugging é uma maneira de ataque através do Bluetooth, geralmente causada por falta de conhecimento, permitindo o acesso indevido ao dispositivo mal configurado.

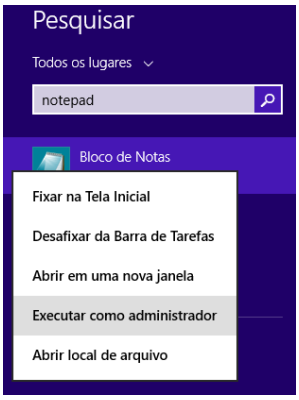
5 - Pharming

5.1 – Conceitos

O termo *pharming* parece ser complicado (talvez pelo nome) mas o conceito é bem simples. Trata-se de um ataque que compromete o serviço de resolução de nomes (DNS), fazendo com que um endereço (URL) seja traduzido para um endereço IP incorreto. Ou seja, você digita um endereço qualquer, o DNS deveria retornar o endereço IP equivalente e o navegador buscaria a página solicitada através desse endereço IP.

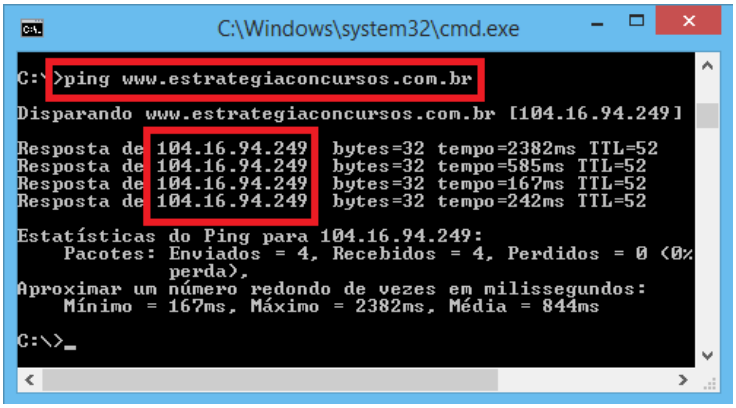
O **comprometimento do DNS** pode ocorrer das seguintes formas:

a) Dispositivo da vítima pode ser infectado por um *malware* que altera o arquivo *hosts* (arquivo destinado a relacionar nomes a endereços IP, geralmente é o primeiro a ser consultado, tanto no Windows como no Linux). Para compreender melhor, faça o seguinte: execute o Bloco de Notas como **Administrador**, abra o arquivo C:\Windows\System32\drivers\etc\hosts, sem extensão mesmo! Procure por Todos os Arquivos (*.*). Abaixo mostro um exemplo:

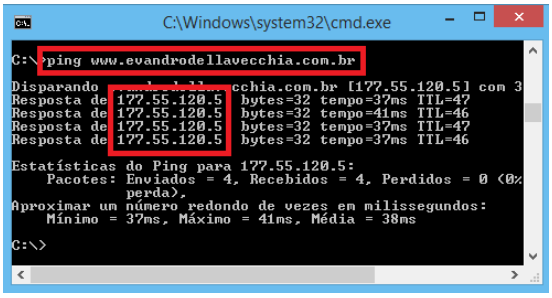


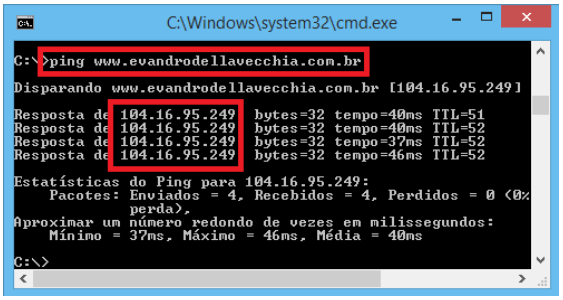


Defini que o endereço IP 104.16.95.249 deve apontar para www.evandrodellavecchia.com.br, porém esse é o endereço IP do servidor responsável pelo armazenamento do sítio do Estratégia Concursos. Como sei disso? Verifique o comando *ping www.estrategiaconcursos.com.br* abaixo.

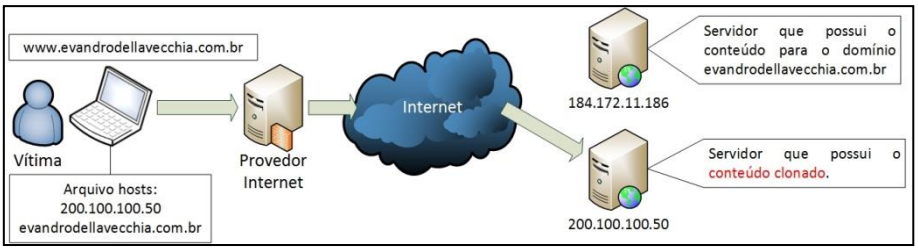


Agora, verifique o comando *ping www.evandrodellavecchia.com.br* abaixo, antes (esquerda) e depois (direita) da alteração do arquivo *hosts*.



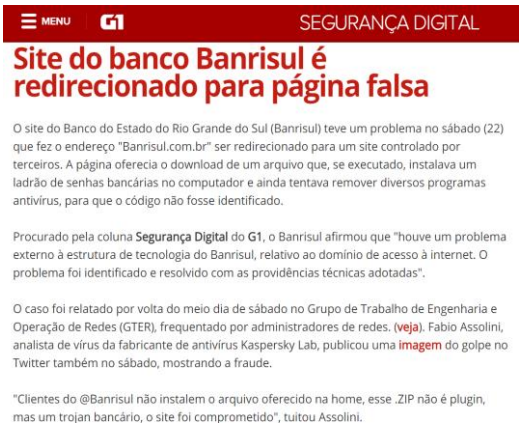


Pronto! Acabei de aplicar *pharming* na minha máquina! Claro que existem outros mecanismos de proteção que impedem que eu acesse uma página através do endereço IP incorreto, mas foge do escopo desta aula. Não esqueça de desfazer as alterações no arquivo *hosts*! Ah...ao tentar alterar o arquivo, seu antivírus pode reclamar e não deixar que você altere, então desative-o por alguns minutos, apenas para testar! Depois, volte tudo ao normal 😊 Para reforçar o conceito de *pharming*, segue uma figura retirada do livro "Perícia Digital – Da investigação à análise forense":



b) O comprometimento pode ocorrer em um servidor DNS que sua máquina consulte, como por exemplo, o servidor DNS utilizado por seu provedor de acesso à Internet. Tal comprometimento pode ocorrer através de um ataque conhecido como ***DNS cache poisoning*** (envenenamento DNS). Tal ataque é realizado através da introdução de dados no *cache* de um servidor DNS que não se originam do servidor de nomes DNS com autoridade real. Resumindo: insere-se dados falsos no servidor DNS. Uma forma de fazer isso é criar e enviar mensagens de atualização falsas em uma grande quantidade e fazer com que o servidor acredite e atualize sua *cache* com os dados falsos.

c) Indo um pouco além, é possível **alterar os dados no servidor DNS raiz**, fazendo com que essas informações sejam replicadas aos servidores que se encontram abaixo, na hierarquia DNS. É um ataque bem mais ousado, mas acreditem, já ocorreu! Abaixo mostro a notícia de 24/10/2016, sobre o banco Banrisul.


MENU G1 SEGURANÇA DIGITAL

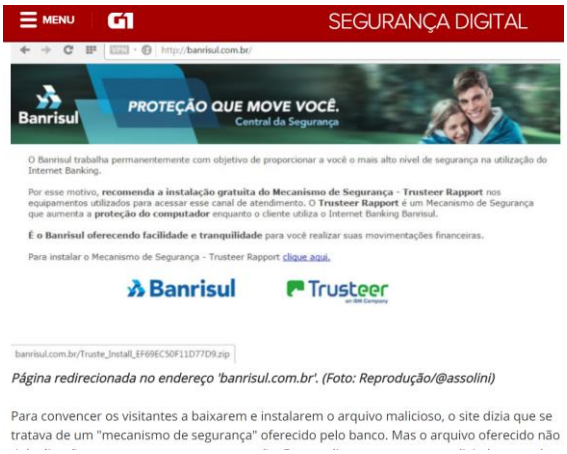
Site do banco Banrisul é redirecionado para página falsa

O site do Banco do Estado do Rio Grande do Sul (Banrisul) teve um problema no sábado (22) que fez o endereço "Banrisul.com.br" ser redirecionado para um site controlado por terceiros. A página oferecia o download de um arquivo que, se executado, instalava um ladrão de senhas bancárias no computador e ainda tentava remover diversos programas antivírus, para que o código não fosse identificado.

Procurado pela coluna **Segurança Digital** do **G1**, o Banrisul afirmou que "houve um problema externo à estrutura de tecnologia do Banrisul, relativo ao domínio de acesso à internet. O problema foi identificado e resolvido com as providências técnicas adotadas".

O caso foi relatado por volta do meio dia de sábado no Grupo de Trabalho de Engenharia e Operação de Redes (GTER), frequentado por administradores de redes. (veja). Fabio Assolini, analista de vírus da fabricante de antivírus Kaspersky Lab, publicou uma imagem do golpe no Twitter também no sábado, mostrando a fraude.

"Clientes do @Banrisul não instalem o arquivo oferecido na home, esse .ZIP não é plugin, mas um trojan bancário, o site foi comprometido", tuitou Assolini.


MENU G1 SEGURANÇA DIGITAL

Banrisul PROTEÇÃO QUE MOVE VOCÊ. Central da Segurança

O Banrisul trabalha permanentemente com objetivo de proporcionar a você o mais alto nível de segurança na utilização do Internet Banking.

Por esse motivo, **recomenda a instalação gratuita do Mecanismo de Segurança - Trusteer Rapport** nos equipamentos utilizados para acessar esse canal de atendimento. O **Trusteer Rapport** é um Mecanismo de Segurança que aumenta a **proteção do computador** enquanto o cliente utiliza o Internet Banking Banrisul.

É o Banrisul oferecendo facilidade e tranquilidade para você realizar suas movimentações financeiras.

Para instalar o Mecanismo de Segurança - Trusteer Rapport clique aqui.

Banrisul Trusteer

Página redirecionada no endereço 'banrisul.com.br'. (Foto: Reprodução/@assolini)

Para convencer os visitantes a baixarem e instalarem o arquivo malicioso, o site dizia que se tratava de um "mecanismo de segurança" oferecido pelo banco. Mas o arquivo oferecido não

Segundo a notícia e a imagem mostrada, ao digitar a URL do banco, uma página clonada era retornada, solicitando que o usuário baixasse e instalasse um "mecanismo de segurança". Porém, tratava-se de um *malware* que capturava as teclas digitadas (*keylogger*). Uma das possibilidades de ter ocorrido esse ataque é a descoberta dos dados de cadastro do domínio no Registro.br (https://registro.br/) e a alteração dos servidores DNS do Banrisul por servidores onde se encontravam a página clonada.

Um conceito adotado pela Cartilha de Segurança para Internet, do CERT.br, é "*Pharming* é um tipo específico de *phishing* que envolve o redirecionamento da navegação do usuário para *sites* falsos, por meio de alterações no serviço de DNS (*Domain Name System*). Neste caso, quando você tenta acessar um *site* legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa".

5.2 – Questões Comentadas

22. (CESPE/TER-RJ - 2012) Pharming é um tipo de golpe em que há o furto de identidade do usuário e o golpista tenta se passar por outra pessoa, assumindo uma falsa identidade roubada, com o objetivo de obter vantagens indevidas. Para evitar que isso aconteça, é recomendada a utilização de firewall, especificamente, o do tipo personal firewall.

Comentários:

Como já vimos, pharming é o redirecionamento para um sítio falso (clonado). Logo, a questão está **errada**.

23. (FUNDEP/IPSEMG - 2013) Analise as seguintes afirmativas acerca de golpes/fraudes na Internet. Em seguida, assinale com V as verdadeiras e com F as falsas.

( ) O pharming é um tipo de golpe que redireciona um usuário para um site falso.

( ) O phishing é um tipo de fraude em que o adversário se utiliza da combinação de meios técnicos e engenharia social para lograr sucesso.

( ) O furto de identidade é quando o adversário tenta se passar por um usuário, em geral, legítimo.

( ) O boato (hoax) é um tipo de golpe em que engenharia social é utilizada eminentemente para invadir computadores alheios.

Assinale a alternativa que apresenta a sequência CORRETA.

A) V V V F.

B) V V F F.

C) F V V F.

D) V F F V.

Comentários:

A única falsa é a última, pois um boato nada mais é do que mensagens alarmantes, solicitando que repassem para muita gente, enchendo as caixas de e-mails e gerando tráfego desnecessário. Logo, a **alternativa A** está correta e é o gabarito da questão.

24. (CESPE/TJ-SE - 2014) Um tipo específico de phishing, técnica utilizada para obter informações pessoais ou financeiras de usuários da Internet, como nome completo, CPF, número de cartão de crédito e senhas, é o pharming, que redireciona a navegação do usuário para sítios falsos, por meio da técnica DNS cache poisoning.

Comentários:

Perfeito! Uma descrição detalhada de pharming, que é um tipo de phishing e uma das formas que ele ocorre é através do envenenamento da cache DNS. Logo, a questão está **correta**.

25. (Quadrix/CRN-3ª Região - 2014) Leia atentamente a seguinte definição.

"Uma tentativa de defraudar os internautas sequestrando o nome do domínio do site ou URL e redirecionando os usuários a um site impostor, no qual são feitas solicitações fraudulentas de informações."

A definição acima refere-se a:

A) Phishing.

B) SPAM.

C) Web Bot.

D) Pharming.

E) Engenharia social.

Comentários:

A palavra-chave da questão é "redirecionando". O usuário pensa que está na página real (inclusive o nome que aparece no navegador está ok), mas na verdade está em uma página clonada! Surgiu uma expressão nova: "Web bot", que pode ser um bot (zumbi) ou o nome de um projeto desenvolvido como um "adivinhador do futuro". Enfim, nada a ver com pharming! Logo, a **alternativa D** está correta e é o gabarito da questão.

26. (FCC/TCE-GO - 2014) Ao tentar entrar em alguns sites de comércio eletrônico para comprar produtos de seu interesse, Maria percebeu que estava sendo redirecionada para sites muito semelhantes aos verdadeiros, mas que não ofereciam conexão segura, nem certificado digital. Pela característica do problema, é mais provável que Maria esteja sendo vítima de

A) vírus.

B) worm.

C) trojan.

D) backdoor.

E) pharming.

Comentários:

Palavra-chave: “redirecionada” = pharming! As demais alternativas mostram malwares de categorias diversas. Logo, a **alternativa E** está correta e é o gabarito da questão.

27. (OBJETIVA/Prefeitura de Cidreira-RS - 2016) É um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Nesse caso, quando o usuário tenta acessar um site legítimo, o seu navegador web é redirecionado, de forma transparente, para uma página falsa. Essa forma de phishing é conhecida como:

A) Boot.

B) EdoRam.

C) Bios.

D) Pharming.

Comentários:

Essa questão é um exemplo de três alternativas absurdas, relacionadas a inicialização da máquina ou tipo de memória RAM e a que sobrou é a correta! Conforme vimos, a cartilha do CERT.br define que pharming é um tipo de phishing que tem o objetivo de redirecionar para um sítio falso. Logo, a **alternativa D** está correta e é o gabarito da questão.

28. (IFSul-MG/IFSul-MG - 2016) De acordo com o CERT.br: “(...) é uma técnica que consiste em alterar campos do cabeçalho de um email, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.”. Considerando um servidor de e-mails configurado erradamente e que um usuário mal-intencionado teve acesso a este servidor para o envio de mensagens com origem forjada, qual foi a técnica utilizada para o envio dessas mensagens?

A) Pharming.

B) Spoofing.

C) Phishing.

D) Spam.

Comentários:

Sempre que a questão falar em falsificar, alterar, etc., fique atento em spoofing. Depois veja se alguma outra também poderia ser a correta. No caso desta questão, não tinha outra alternativa semelhante. Logo, a **alternativa B** está correta e é o gabarito da questão.

29. (FCC/TRF-3ª Região - 2016) Para responder a questão considere as informações abaixo.

Os Técnicos Judiciário de TI de um Tribunal têm ciência sobre ataques da internet e por isso adotam medidas de defesa contra (I) falsificação de e-mail porque esta técnica consiste em alterar (II) elementos do e-mail de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. O que possibilita esta técnica de falsificação é a característica de um (III) protocolo de Internet que permite que campos do From, do Reply to e do Return-Path sejam adulterados. Isto é bastante usado por alguns hackers para propagação de códigos maliciosos, envio de spam e (IV) tipos de ataques que atuam informando, falsamente, que a não execução dos procedimentos descritos pode acarretar sérias consequências, como, por exemplo, a inscrição em serviços de proteção de crédito e coisas semelhantes.

O nome pelo qual a falsificação referida em I é conhecido e os elementos do e-mail alterados referidos em II correspondem, correta e respectivamente, a e-mail

A) pharming e texto da mensagem.

B) splashing e dados do remetente.

C) spoofing e campos do cabeçalho.

D) brut force e dados do destinatário.

E) defacement e campos do cabeçalho.

Comentários:

Novamente, as palavras alterar ou falsificar indicam o spoofing. Como se trata de falsificação, alteram-se os campos do cabeçalho (remetente, destinatário, etc.) e não o corpo do e-mail. Logo, a **alternativa C** está correta e é o gabarito da questão.

30. (FUNDATEC/IGP-RS - 2017) Peritos criminais da Seção de Computação Forense foram designados para realizar exame na rede de computadores de uma empresa que estaria sendo alvo de crimes cibernéticos. Enquanto estava ocorrendo o suposto ataque, os peritos criminais coletaram o tráfego de rede do local examinado. Nesses vestígios coletados, os peritos criminais identificaram pacotes que eram direcionados para um DNS que não era de uma autoridade real; sempre que os usuários tentavam acessar a página na internet de um determinado banco, eram redirecionados para uma página de escolha do criminoso. Analisando o servidor de DNS, os peritos constataram que foi adicionado um registro de DNS falso no cache do servidor de DNS que redirecionava os usuários para sites falsos. Com base nos fundamentos de investigação em redes de computadores, assinale a alternativa que explica o redirecionamento de DNS e a provável técnica utilizada pelos criminosos.

A) Os criminosos usaram a técnica de envenenamento de DNS ou DNS Poisoning.

B) A técnica utilizada pelos criminosos é conhecida como DNS oculto ou DNS redirection.

C) Este é um caso clássico em que o criminoso utilizou de injeção de SQL ou SQL injection.

D) Os vestígios coletados pelos peritos criminais apontam para uma técnica conhecida como roubo de sessão ou DNS session injection.

E) O registro de DNS falso no cache do servidor indica que os criminosos utilizaram um ataque de negação de serviço ou Denial of Service (DoS), que fez com que todos os usuários que tentavam acessar a internet fossem redirecionados para um servidor de DNS do criminoso.

Comentários:

O trecho "Analisando o servidor de DNS, os peritos constataram que foi adicionado um registro de DNS falso no cache do servidor de DNS que redirecionava os usuários para sites falsos." deixa claro que houve um envenenamento da cache DNS! Logo, a **alternativa A** está correta e é o gabarito da questão.

31. (UFMT/UFSBA - 2017) Phishing é o tipo de fraude na internet, por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social. Sobre esse assunto, analise as afirmativas.

I - Pharming é um tipo específico de phishing que envolve o redirecionamento da navegação do usuário para sites falsos, de forma que, quando ele tenta acessar um site legítimo, o navegador Web é redirecionado para uma página falsa.

II - Por se tratar de uma fraude pouco comum e, na maioria das vezes, inofensiva, descarta-se a utilização de mecanismos de segurança, como programas antimalware, firewall pessoal e filtros antiphishing.

III - Sites de comércio eletrônico ou Internet Banking confiáveis, na maioria das vezes, utilizam conexões seguras, por exemplo HTTPS, quando dados sensíveis são solicitados.

IV - O phishing pode ocorrer por meio do envio de mensagens eletrônicas que tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular.

Estão corretas as afirmativas.

A) I e IV, apenas.

B) II e III, apenas.

C) II, III e IV, apenas.

D) I, III e IV, apenas.

Comentários:

Todas estão redondinhas, com exceção da (II) phishing é muito comum de acontecer e mecanismos de segurança não são descartados, principalmente os filtros antiphishing! Logo, a **alternativa D** está correta e é o gabarito da questão.

32. (CESPE/Polícia Federal - 2018) Um tipo de ataque contra o serviço DNS é o pharming, que envolve o redirecionamento do navegador do usuário para sítios falsos por meio da técnica conhecida como envenenamento de cache DNS.

Comentários:

Como vimos na aula, o comprometimento do DNS pode ocorrer através de um ataque conhecido como DNS cache poisoning (envenenamento DNS). Tal ataque é realizado através da introdução de dados no cache de um servidor DNS que não se originam do servidor de nomes DNS com autoridade real. Resumindo: insere-se dados falsos no servidor DNS. Uma forma de fazer isso é criar e enviar mensagens de atualização falsas em uma grande quantidade e fazer com que o servidor acredite e atualize sua cache com os dados falsos. Logo, a questão está **correta**.

33. (UNEMAT/UNEMAT - 2018) Pharming é uma ameaça de segurança do tipo phishing, que tem o intuito de direcionar o usuário para sites falsos, por meio de alterações no servidor de DNS.

Cartilha de Segurança para Internet, versão 6.0 / CERT.br - São Paulo: Comitê Gestor da Internet no Brasil, 2017.

Considerando este tipo de ataque, analise as asserções a seguir e a relação entre elas.

I. Usuários que informam o endereço URI (Universal Resource Identifier) na barra do navegador evitam ataques do tipo Pharming.

II. Usuários que informam o endereço URL (Universal Resource Locator) na barra do navegador evitam ataques do tipo Pharming.

III. Visando mitigar ameaça do tipo Pharming, o administrador de redes deve instruir o usuário a inspecionar se o certificado se segurança é valido e corresponde a instituição proprietária do site, quando utilizado o protocolo HTTPS.

IV. Quando o usuário acessa o endereço legítimo de um site em seu navegador web, sua requisição será redirecionada, de maneira transparente, para uma página falsa.

Sobre o exposto assinale a alternativa que apresenta as afirmações corretas.

A) I e II.

B) II e III.

C) I e IV.

D) II e IV.

E) III e IV.

Comentários:

(I e II) URI (Uniform Resource Identifier) é uma string que identifica de forma única um determinado recurso. URL (Uniform Resource Locator) é uma URI que especifica o significado de um recurso, especificando qual o acesso primário e a localização na rede. Ex.: a URL https://estrategiaconcursos.com.br/teste se refere a um recurso /teste representado na forma de HTML e a localização é obtida através do protocolo HTTPS em um host com o domínio estrategiaconcursos.com.br. Logo, as afirmativas I e II estão incorretas. (III) Correta, pois mesmo que utilize o HTTPS pode haver um sítio clonado, utilizando uma certificação de outra empresa (ex.: sítio do Banco do Brasil clonado, utilizando um certificado em nome de BB2 - tentando induzir a vítima ao erro, ao verificá-lo); (IV) Correta, na barra de endereço estará tudo ok, mas "por baixo dos panos" a tradução para o endereço IP direcionará para o local errado. Logo, a **alternativa E** está correta e é o gabarito da questão.

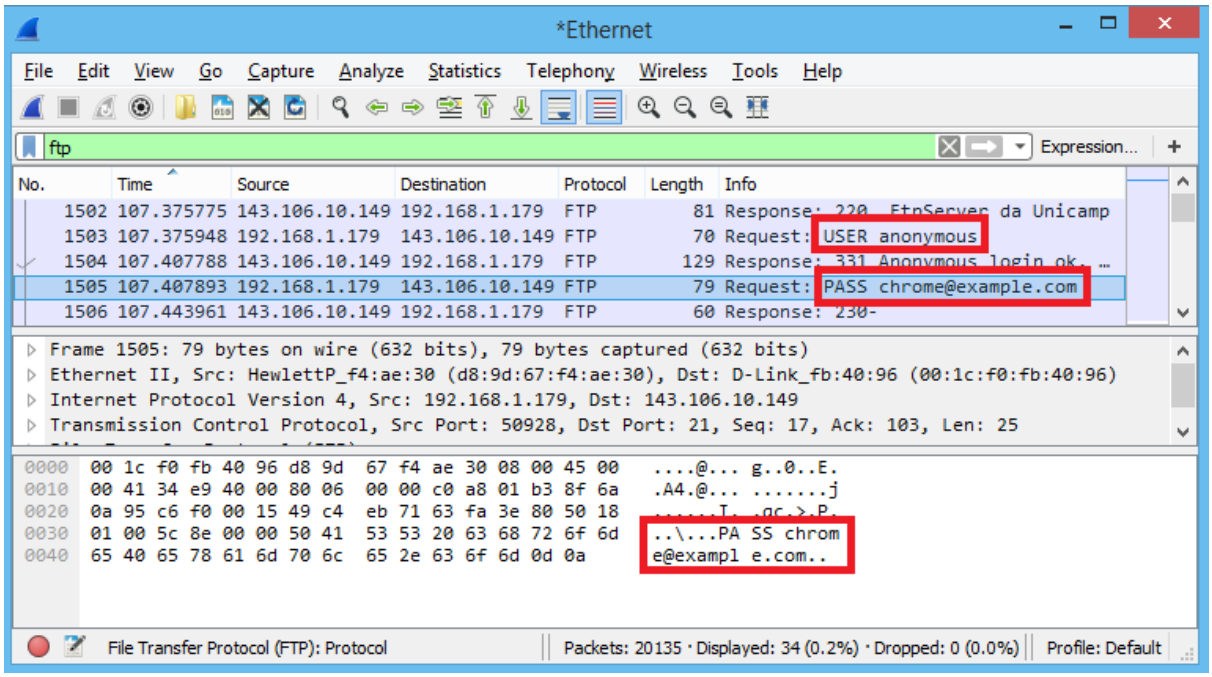
6 - Sniffer

6.1 – Conceitos

Um *sniffer* tem a finalidade de capturar pacotes que **chegam até uma interface de rede** (placa de rede) de um dispositivo. Por padrão, as interfaces de rede descartam os pacotes que não são destinados ao dispositivo (endereço MAC do dispositivo ou *broadcast*), porém os *sniffers* possuem a capacidade de ativar o **modo promíscuo** de uma interface, o que permite **capturar todos os pacotes**, incluindo os não endereçados a ele.

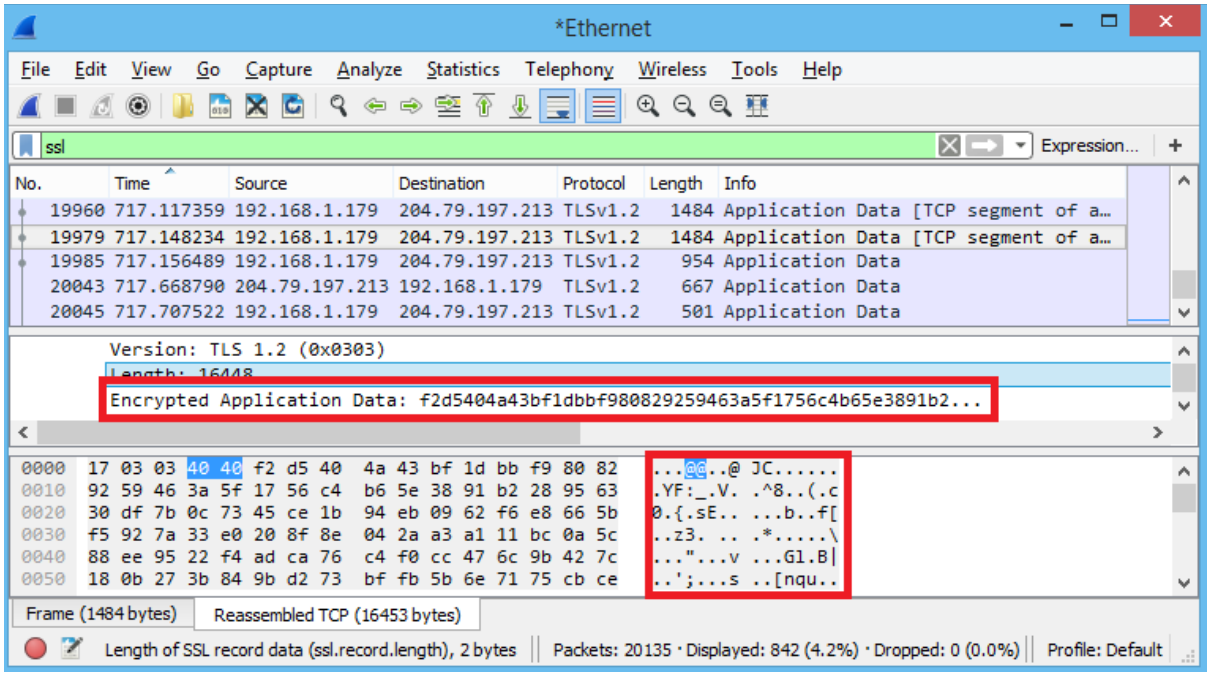
Diferente da maioria dos ataques, trata-se de um **ataque passivo**, pois "escuta" tudo o que chega a seus "ouvidos" e, depois, esses dados podem ser analisados. Mas é possível capturar uma senha, por exemplo? Claro! Se ela estiver cifrada, não é possível visualizá-la de imediato, mas é possível tentar decifrá-la, o que pode ser uma tarefa muito demorada, conforme veremos em aula futura deste curso. Mas, se a senha estive "em claro", bingo! Você poderá visualizá-la instantaneamente!

Para entender melhor, sugiro que você instale um *sniffer*, como o *tcpdump* ou o *Wireshark*. As questões que mostram os pacotes capturados por um *sniffer*, cobram conhecimento dos protocolos, então é importante você dominar os protocolos cobrados em seu edital. Abaixo segue um exemplo de pacotes do protocolo FTP, o qual não criptografa seus dados. Note que é possível visualizar o usuário e a senha!



Para melhorar a visualização, é possível utilizar filtros: eu coloquei “ftp”. Note que foi realizada uma conexão com um servidor FTP da Unicamp (ftp://ftp.unicamp.br/), com o usuário *anonymous* e a senha *chrome@example.com*. Trata-se de um usuário e senha padrão para esse servidor, apenas para demonstrar, mas poderia ser um usuário *root*!

Por esses motivos, dados sensíveis devem ser cifrados. Não é à toa que instituições financeiras e sítios de comércio eletrônico utilizam protocolos com criptografia, em especial o HTTPS (HTTP sobre SSL/TLS). Abaixo é mostrada uma captura de pacotes SSL, com destaque aos dados cifrados. Não é possível entender nada!



Segundo Nakamura, mesmo sendo um ataque passivo, existem técnicas para detectar se um *sniffer* está em execução em um segmento de rede, sendo as duas primeiras não muito efetivas:

a) O administrador pode verificar em cada equipamento os processos em execução e as interfaces em modo promíscuo, o que se torna trabalhoso, e, se for um processo executado por um *cracker*, pode estar escondido (não mostrado na lista de processos nem como interface em modo promíscuo);

b) Utilização de uma "isca" contendo dados chamativos, como o tráfego de senhas; se o cracker tentar utilizá-las em algum momento significa que ele utilizou um *sniffer*;

c) **MAC *detection***: tira proveito de um erro na implementação do TCP/IP de diversos sistemas operacionais, os quais utilizam **apenas o endereço IP** para entregar os pacotes, **não conferindo o endereço MAC** quando a interface está em modo promíscuo. Assim, a técnica utiliza pacotes ICMP *echo request* (*ping*) com o endereço IP de um host, mas com um endereço MAC falso; se houver *sniffer* em execução, o endereço MAC não será conferido e responderá o *ping*. Assim você descobre o bisbilhoteiro!

d) ***Load detection***: supõe-se que equipamentos que executam *sniffers* possuem maior processamento, e consequentemente, levam **mais tempo para responder**; essa técnica faz uma análise estatística dos tempos de resposta com pouco tráfego na rede e com o tráfego a ser capturado pelos sniffers; os tempos são comparados e se a diferença for grande, há a suspeita do uso de um *sniffer*.

6.2 – Questões Comentadas

34. (CESPE/Polícia Federal - 2004) A captura de pacotes que trafegam na rede com uso de um sniffer é um exemplo de ataque para o qual não há nenhuma forma de detecção possível pelo administrador de rede.

Comentários:

Quando aparece "nenhuma", desconfie! Há algumas formas sim, tais como MAC detection e load detection. Logo, a questão está **errada**.

35. (CESPE/TJ-AL - 2012) As técnicas que realizam a detecção remota de sniffers na rede sem acessar cada equipamento do segmento de rede são

A) coordinated scans e DNS detection.

B) MAC detection e load detection.

C) DNS detection e dumpster diving.

D) decoy e MAC intrusion.

E) fail detection e load detection.

Comentários:

A questão deixa claro que não deve ter o acesso a cada equipamento. Então só pode ser MAC detection e load detection. Logo, a **alternativa B** está correta e é o gabarito da questão.

36. (AOCP/TCE-PA - 2012) Servidores conectados à Internet estão sujeitos a vários tipos de ataques. São alguns desses tipos de ataques, apenas:

A) DoS, flood, trojan.

B) vírus, trojan e adware.

C) backdoor, waf, sniffer.

D) phishing, flood, spoofing.

E) vírus, sniffer, keylogger.

Comentários:

(A) Trojan é um malware; (B) todos são malware; (C) backdoor é um malware; **(D) todos são ataques!** (E) vírus e keylogger são malwares.

37. (FCC/TRT-5ª Região - 2013) Há diversas técnicas e práticas utilizadas para monitoramento e análise de tráfego de dados nas redes. Considere:

I. É uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos. Pode ser utilizada por administradores de redes, de forma legítima, para detectar problemas, analisar desempenho e monitorar atividades maliciosas ou por atacantes, de forma maliciosa, para capturar informações como senhas, números de cartão de crédito e conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

II. Prática que pode ser utilizada por provedores de acesso à internet com o objetivo de limitar o tamanho da banda para os protocolos e programas que usam mais a rede, notadamente os de transferência de arquivos grandes, como P2P. Alguns provedores limitam, inclusive, a transmissão de arquivos via FTP. Esta prática é realizada para garantir que os usuários, que não utilizam esses protocolos de transferência ou não fazem downloads de grandes arquivos, possam ter acesso a outros tipos de serviço sem enfrentar lentidão na rede, embora seja condenada por algumas instituições protetoras dos direitos do consumidor.

As descrições I e II referem-se, respectivamente, a

A) IDS e NAT.

B) traffic shaping e sniffer.

C) NAT e VoIP.

D) sniffing e traffic shaping.

E) IDS e Torrent.

Comentários:

Sniffing já falamos bastante, tranquilo...e traffic shapping é a técnica de delimitar a banda de acordo com o tipo de tráfego, algo que foi proibido pela lei denominada "Marco Civil da Internet", mas será que estão respeitando? Logo, a **alternativa D** está correta e é o gabarito da questão.

38. (CESPE/MS - 2013) O sniffer, que pode ser do tipo filtro de pacotes e do tipo proxy de aplicações, é um dispositivo que tem por objetivo aplicar uma política de segurança a determinado ponto de uma rede de computadores.

Comentários:

Se fosse firewall, a questão estaria correta, mas como menciona sniffer...está **errada**!

39. (Quadrix/CRO-GO - 2013) Como é chamado o software capaz de interceptar e registrar o tráfego de dados em uma rede de computadores?

A) Vírus

B) Trojan.

C) Sniffer.

D) Worm.

E) Spyware.

Comentários:

Essa foi fácil, heim? Tirando o sniffer, os demais são malwares. Logo, a **alternativa C** está correta e é o gabarito da questão.

40. (FCC/TJ-AP - 2014) Um especialista em segurança de redes desconfia que uma aplicação está sendo muito utilizada e está diminuindo a capacidade dos recursos de rede. Para comprovar suas suspeitas resolveu utilizar um sniffer de rede muito popular que pode ser utilizado em redes Unix e Windows para analisar os pacotes recebidos e transmitidos por qualquer interface de rede, sendo possível aplicar vários tipos filtros. Este sniffer é conhecido como

A) Asterisk.

B) Vyatta.

C) Everest.

D) Wireshark.

E) NDISwrapper.

Comentários:

Mais uma que pede o Wireshark! Existiam versões para Windows, Linux, MAC. Acessando o sítio do Wireshark neste ano, só vi download para Windows e MAC. Mas garanto que existem versões para Linux também, pois já usei 😊. Logo, a **alternativa D** está correta e é o gabarito da questão.

41. (CESPE/Telebras - 2015) Sniffers são programas aparentemente inofensivos cuja principal característica é utilizar a técnica de mascaramento. A técnica em questão permite, por exemplo, que um sniffer seja anexado a um jogo, que, por sua vez, ao ser instalado em um computador, coletará informações bancárias do usuário.

Comentários:

Nada de mascaramento! Sniffer serve para capturar tráfego! Logo, a questão está **errada**.

42. (FGV/CODEBA - 2016) No contexto do correio eletrônico, muitas vezes um tipo de mensagem chega ao usuário sem que ele tenha solicitado ou considerado a hipótese de recebê-la. Essas mensagens são transmitidas e inseridas com finalidade comercial, tentando fazer com que a pessoa adquira algum produto ou serviço. Essas mensagens são conhecidas por

A) swap.

B) sniffer.

C) scrum.

D) spoof.

E) spam.

Comentários:

Mensagens indesejadas, não solicitadas indicam spam! Swap é aquela troca realizada entre a memória RAM e a memória virtual. Scrum é uma metodologia ágil, nada a ver com a questão! Logo, a **alternativa E** está correta e é o gabarito da questão.

43. (FCC/TRF-3ª Região - 2016) Um usuário que se conecta em uma rede wifi em um local público, por exemplo, está exposto a vários tipos de ataques Man in The Middle – MITM. Nesse sentido, para tomarem alguma ação preventiva, os Técnicos Judiciários de TI do TRF3 devem estar atentos a um desses tipos de ataque, o Session Hijacking, que é utilizado para o sequestro de sessão por meio de

A) modificação do channel Cain & Abe

B) roubo de cookie que utiliza HTTP.

C) envenenamento do cache HTTP.

D) interceptação do tráfego da rede para capturar uma consulta DNS.

E) sequestro do ettercap, via sniffer.

Comentários:

O sequestro de sessão é possível, dentre outras formas, através do roubo de um cookie HTTP, pois nele a sessão permanece aberta, enquanto não expirar. Como você acha que pessoas acessam contas do Gmail de outras que fecharam o navegador sem realizar o devido logoff? Logo, a **alternativa B** está correta e é o gabarito da questão.

44. (IBFC/EBSERH - 2016) Para o gerenciamento de rede, monitoramento e diagnóstico de ambientes computacionais, muitas vezes, utiliza-se uma ferramenta, constituída de um software ou hardware, que é capaz de interceptar e registrar o tráfego de dados em uma rede de computadores denominado tecnicamente de:

A) jitter

B) sniffer

C) ping

D) gateway

E) noise

Comentários:

Mais uma questão bem objetiva. Jitter é uma variação estatística do atraso na entrega de dados em uma rede; Ping é aquela ferramenta clássica para ver se uma máquina está "viva"; Gateway é a máquina que fica na "borda" da rede, é o "portão" de entrada/saída; Noise? É barulho 😊. Logo, a **alternativa B** está correta e é o gabarito da questão.

45. (FCC/TRF-5ª Região - 2017) Os Sniffers de rede podem ser ferramentas adequadas para monitorar o tráfego da rede local. Para aumentar a eficiência do Sniffer deve-se utilizá-lo no modo promíscuo em que

A) apenas os pacotes endereçados para um servidor são monitorados.

B) pacotes criptografados são decifrados e analisados.

C) pacotes são gerados aleatoriamente para analisar a correta configuração do switch.

D) todos os pacotes que trafegam pela rede local são monitorados.

E) responde automaticamente a todos os pacotes de verificação de estado da rede.

Comentários:

Como já vimos, em modo promíscuo todos pacotes que chegam à interface de rede são recebidos, mesmo aqueles não destinados à máquina. A afirmativa mais correta é a D, mas se um switch é utilizado na rede local, ela não seria a alternativa correta (nenhuma seria!). Fique ligado, esse é o modus operandi da FCC! Sempre procure a mais correta ou a menos errada, quando se trata dessa banca. Logo, a **alternativa D** está correta e é o gabarito da questão.

46. (UPENET/IAUPE/UPE - 2017) Uma das ferramentas mais poderosas para gerenciar o funcionamento de uma rede de computadores é um sniffer. Qual dos abaixo é um sniffer?

A) Traceroute

B) Wireshark

C) Ping

D) Netstat

E) SystemMonitor

Comentários:

Fácil! Geralmente citam o Wireshark ou o TCP dump. Não esqueça! Logo, a **alternativa B** está correta e é o gabarito da questão.

47. (UFU-MG/UFU-MG - 2018) Em um equipamento rodando Linux, o comando tcpdump é um dos mais, se não o mais, "famoso" sniffer para sistemas GNU/Linux. Com ele, podemos realizar análises e solucionar problemas. O comando tcpdump permite aos administradores a capacidade de monitorar

A) desempenho do servidor.

B) desempenho da aplicação.

C) tráfego e atividade da rede.

D) arquivos e diretórios.

Comentários:

Como vimos na aula, através do tcpdump ou de qualquer outro sniffer é possível que os administradores monitorem os pacotes de dados trafegados pela rede. Não é papel de um sniffer monitorar o desempenho de um computador, aplicação ou ainda seus dados (arquivos, diretórios, etc.). Logo, a **alternativa C** está correta e é o gabarito da questão.

48. (FGV/Banestes - 2018) Com relação ao uso de sniffers, analise as afirmativas a seguir:

I. Um sniffer costuma ser utilizado para encontrar outros sniffers presentes em outras máquinas na rede.

II. Podem ser utilizados como fonte de negação de serviço na sub-rede onde operam.

III. A interface de rede deve estar operando em modo promíscuo para que um sniffer funcione adequadamente.

Está correto somente o que se afirma em:

A) I;

B) II;

C) III;

D) I e II;

E) II e III.

Comentários:

(I) Sniffer atua de forma passiva, apenas captura os pacotes de dados; (II) Se atua, de forma passiva, não podem desferir ataques de DoS; (III) Perfeito! Tem que operar em modo promíscuo, que por sua vez depende de permissão de administrador. Logo, a **alternativa C** está correta e é o gabarito da questão.

49. (CESPE/Polícia Federal - 2018) Um dos objetivos do firewall é monitorar todo o tráfego de dados entrando e saindo de uma rede local e entrar em ação ao identificar um sniffer externo.

Comentários:

Um sniffer atua de forma passiva, apenas capturando pacotes de dados, sem transmiti-los. Logo, um firewall não poderia detectar um sniffer. Logo, a questão está **errada**.

7 - Negação de Serviço (DoS/DDoS)

7.1 – Conceitos

Ataques de negação de serviço têm o objetivo de **interromper atividades legítimas**, como servidores de páginas Web, servidores de correio eletrônico, entre outros. Uma maneira de provocar ataques de DoS é através da **exploração de vulnerabilidades** presentes no dispositivo ou em algum software da vítima. Digamos que o atacante descubra que a vítima possui um servidor de e-mail X, versão Y e sabe que tal versão possui uma vulnerabilidade que, ao enviar determinados pacotes malformados, ele simplesmente trava, tornando-se necessária a reinicialização do servidor.

Parece complicado, certo? Errado! Existem bases públicas de vulnerabilidades conhecidas. Então, após saber ou ter alguma ideia da versão de um serviço que a vítima possui, o atacante pode pesquisar se ela possui alguma vulnerabilidade e, para facilitar, se existe algum *exploit* (*software* ou pedação de software que explora uma *vulnerabilidade*) pronto! Um sítio muito utilizado para a pesquisa de vulnerabilidades conhecidas é o CVE (https://cve.mitre.org/):



Note que uma simples consulta pela expressão “dos” encontrou 1847 ocorrências, em 23/03/2018. Na figura são mostradas apenas as quatro primeiras vulnerabilidades listadas, todas descobertas em 2018.

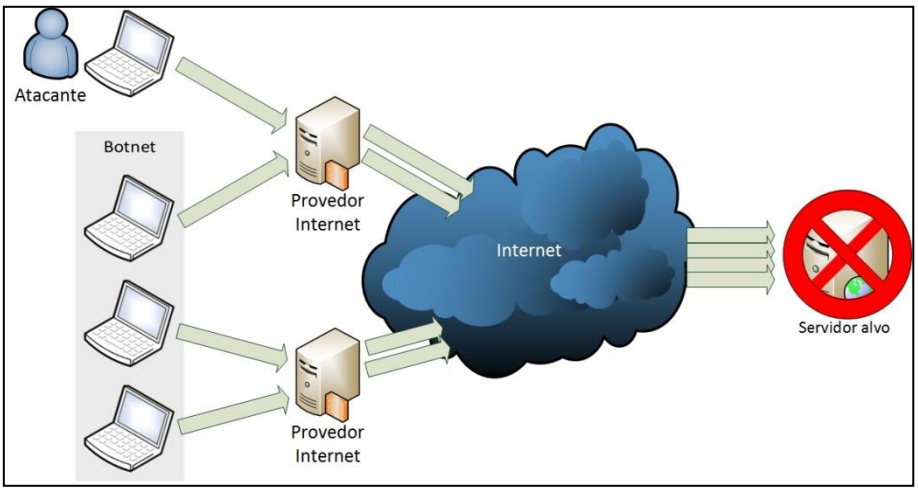
Outra maneira, a mais conhecida, é enviar um grande número de requisições ao alvo, fazendo com que haja um esgotamento de recursos do dispositivo/rede: uso excessivo do processador, memória, banda da rede, etc.; ou do software: sistema operacional ou a própria aplicação servidora. Ou seja, DoS não se trata de uma invasão, trata-se da inutilização (ou lentidão extrema) de um serviço por um período de tempo.

O ataque distribuído de negação de serviço (**DDoS - *Distributed Denial of Service***) consegue êxito excedendo os limites de recursos do alvo através de requisições enviadas de diversos dispositivos simultaneamente.

Para isso, pode-se combinar com várias pessoas ao mesmo tempo (através de um grupo de Whatsapp, por que não?) ou através de *botnets* (máquinas "zumbis", assunto a ser tratado ainda nessa aula).

Por se tratar de centenas ou milhares de computadores realizando o ataque, o DDoS possui uma melhor eficácia que o DoS. Fica difícil combatê-lo, pois os responsáveis pela segurança do servidor não conseguem estabelecer critérios/regras para bloquear todos os acessos/requisições que causam transtorno.

A figura abaixo, retirada do livro "Perícia Digital – Da investigação à análise forense", mostra um cenário de ataque DDoS, partindo de um atacante em conjunto com uma *botnet*, tendo o objetivo alcançado: tornar o dispositivo ou uma aplicação deste inoperante.



Uma forma "indireta" desse tipo de ataque é (D)DoS **refletivo**, que ocorre quando um atacante envia requisições com o **endereço IP origem falsificado a um servidor**. O servidor responde ao endereço IP falso, que na verdade é o alvo do ataque!

7.2 – Questões Comentadas

50. (FGV/AL-BA - 2014) Considere que um hacker comprometa milhares de hosts ao redor do mundo, criando uma botnet com intenção maliciosa. Em determinada ocasião, comandados por um computador mestre, estes hosts executam um ataque conjunto a um determinado servidor web ou DNS, consumindo a largura de banda do servidor e comprometendo seu funcionamento. O cenário descrito é típico de um ataque denominado

A) worms.

B) spoofing.

C) phishing.

D) DDoS

E) DoS.

Comentários:

Veremos em seguida que uma botnet geralmente é utilizada para ataques, incluindo o DDoS. Logo, a **alternativa D** está correta e é o gabarito da questão.

51. (CESPE/MEC - 2015) No que se refere aos ataques de negação de serviço, julgue o item que se segue. Nesse sentido, considere que a sigla DDoS, sempre que utilizada, se refere ao ataque Distributed Denial of Service.

Ataques Xmas-DDoS (christmas tree packets) são caracterizados pela inundação de pacotes ICMP tipo 8 em uma rede de dados.

Comentários:

XMAS (Christmas) é uma alusão à árvore de Natal (três luzes ligadas e as demais desligadas (coisa de nerd!). As flags do TCP ligadas são FIN, PSH e URG. Logo, não há o que se falar em ICMP! Logo, a questão está **errada**.

52. (CESPE/MEC - 2015) Ataques refletivos de DDoS de NTP têm como objetivo indisponibilizar os serviços de NTP pelo mundo, atrasando-os em uma hora, o que gera inconsistências nos horários registrados pelos logs e nas trocas de mensagens.

Comentários:

Por que o atraso seria de exatamente uma hora? 😊 Questão sem pé nem cabeça! A questão está **errada**.

53. (FCC/TRT-3ª Região - 2015) O Administrador de uma rede local de computadores, que utiliza IPs Classe B, identificou que o servidor da rede local recebeu requisições de acesso de um computador da mesma rede local com IP: 192.168.1.1. O tipo de ataque identificado é conhecido como

A) DoS.

B) Spoofing.

C) Scanning.

D) Defacement.

E) DDoS.

Comentários:

A questão exige conhecimento de redes. Vamos lá, a rede 192.168.1.0, por padrão, pertence à classe C. Se a rede local utiliza classe B, tem algo errado, não? Pois é, pelas alternativas mostradas, pode ser uma falsificação de endereço IP, ou seja, spoofing! Logo, a **alternativa B** está correta e é o gabarito da questão.

54. (VUNESP/TCE-SP - 2015) Existem diferentes tipos de ataques de hackers por meio das redes de computadores. Nesse contexto, o ataque no qual vários computadores realizam requisições ou enviam pacotes malformados para um sistema pela rede é denominado

A) DoS.

B) DDoS.

C) Flooding.

D) Phishing.

E) Spoofing.

Comentários:

Existem servidores que ao receber pacotes malformados, travam, causando negação de serviço. Como a questão fala em vários computadores, estamos diante de um DDoS. Logo, a **alternativa B** está correta e é o gabarito da questão.

55. (IDIB/Prefeitura de Limoeiro do Norte-CE - 2016) São ameaças de Internet, EXCETO

A) Malware.

B) Criptografia.

C) DdoS.

D) Negação de Serviço.

Comentários:

Criptografia é uma forma de proteção da confidencialidade! Jamais seria uma ameaça! Logo, a **alternativa B** está correta e é o gabarito da questão.

56. (CESPE/TRT-7ª Região - 2017) O ataque que amplia o número de acessos a um servidor, gerando indisponibilidade de recursos aos usuários, é denominado

A) phishing.

B) DoS.

C) spoofing.

D) adware.

Comentários:

Ampliar o número de acessos = aumentar a carga no alvo, tentando fazer com que ele não consiga suportar o processamento, muitas vezes através de flooding. Logo, a **alternativa B** está correta e é o gabarito da questão.

57. (FCC/Prefeitura de Teresina-PI - 2016) Trata-se de um tipo de ataque em redes de computadores que compreende a ação de um Botnet que concede o controle de vários computadores para enviar constantemente pacotes de dados a um determinado servidor. O tipo de ataque descrito é

A) Spoofing.

B) DDoS.

C) Phishing.

D) DoS.

E) Spam.

Comentários:

Novamente, botnet com vários computadores enviando pacotes a um único alvo! Logo, a **alternativa B** está correta e é o gabarito da questão.

58. (CESGRANRIO/UNIRIO - 2016) Um ataque de DDoS (Distributed Denial of Service) visa a consumir os recursos do alvo em larga escala para provocar uma sobrecarga que prejudique o fornecimento do serviço. Quando esse ataque é classificado como DDoS refletor, os zumbis escravos geram pacotes, com uma solicitação de resposta, que

A) são destinados aos próprios zumbis escravos para amplificar o ataque ao alvo.

B) são destinados aos zumbis mestres que, por sua vez, os repassam para o alvo.

C) possuem seus próprios endereços no campo de origem dos pacotes.

D) possuem o endereço do alvo no campo de origem dos pacotes.

E) possuem os endereços dos zumbis mestres no campo de origem dos pacotes.

Comentários:

Um ataque DDoS refletivo funciona da seguinte forma: requisições são enviadas a um servidor, com o endereço IP origem falso. Esse endereço falso é na verdade o alvo que se quer atingir. O servidor responde todas requisições para o endereço IP falso. O atacante não recebe nenhuma resposta! Logo, a **alternativa D** está correta e é o gabarito da questão.

59. (FCC/DPE-RS - 2017) O tipo de ataque DDoS - Distributed Denial of Service que explora a vulnerabilidade do processo de comunicação do protocolo TCP é o

A) SYN Flood.

B) NTP Flood.

C) Ping of Death.

D) UDP Flood.

E) VoIP Flood.

Comentários:

A única alternativa relacionada ao TCP é a "SYN Flood", pois SYN é uma flag do TCP. O ping utiliza ICMP, NTP e VoIP utilizam UDP. Logo, a **alternativa A** está correta e é o gabarito da questão.

60. (IBFC/Polícia Científica-PR - 2017) O "ping da morte" (ping of death) é um ataque que objetiva a indisponibilidade de servidores por meio do envio maciço de pacotes de ping malformados. Um ataque dessa categoria é classificado como:

A) Worm

B) Ransomware

C) Backdoor

D) Spyware

E) DoS/DDoS

Comentários:

Mais uma vez, pacotes malformados...e ainda facilitou, colocando DoS/DDoS na mesma alternativa 😊. Logo, a **alternativa E** está correta e é o gabarito da questão.

61. (CESPE/ABIN - 2018) Os testes CAPTCHA são eficientes contra os ataques DDoS volumétricos e os de exaustão das conexões TCP, mas são inócuos contra os ataques DDoS de camada de aplicação.

Comentários:

Ataques volumétricos (inundação) não possuem conexão, os pacotes são simplesmente enviados em grande quantidade, sem passar pela camada de aplicação, onde se encontram os captchas! Logo, q questão está **errada**.

62. (CESPE/FUB - 2018) O principal objetivo de um ataque DDoS é causar superaquecimento e danos físicos ao hardware do processador da máquina-alvo, por meio do envio simultâneo de um volume muito grande de requisições de conexão a partir de milhares de máquinas distribuídas.

Comentários:

Como vimos o principal objetivo do ataque de negação de serviço (distribuído ou não) é tornar um serviço indisponível ou dificultar seu funcionamento. Isso não necessariamente implica em superaquecimento ou danos físicos (embora possa ocorrer, é raro). Logo, a questão está **errada**.

8 - Softwares Maliciosos (Malwares)

8.1 – Conceitos

A primeira palavra que vem à mente quando se fala em software malicioso é vírus, e por consequência, o software antivírus, o responsável por tentar eliminá-lo. Porém, a criatividade do ser humano é tão grande, que surgiram diversas pragas virtuais, com características diferentes. Conforme essas características, dezenas de categorias de *malwares* foram criadas e são esses nomes, muitas vezes "estranhos", que são cobrados em provas de concurso! Vejamos...

Vírus

As principais características dessa categoria são: a necessidade de execução para entrar em atividade e a realização de cópia de si próprio para novos arquivos ou agregando a outros arquivos (arquivos hospedeiros). Ou seja, se você receber um vírus em um e-mail, o simples fato de abrir e ler o e-mail não significa que você tenha sido infectado! Mas se você bancar o curioso e executar o arquivo "fotos.exe", aí podemos ter um problema... ☺

Um vírus não precisa ser um arquivo executável, pode ser um vírus de macro, por exemplo. Macro é uma sequência de comandos que pode ser armazenada em um documento de texto ou planilha eletrônica, por exemplo. O Word permite o uso de macros e uma definição/propaganda copiada do sítio da Microsoft (https://support.office.com/pt-br/article/criar-ou-executar-uma-macro-c6b99036-905c-49a6-818a-dfb98b7c3c9c) é:

> *Para poupar tempo em tarefas que você costuma realizar com frequência, compacte as etapas em uma macro. Em primeiro lugar, grave a macro. Em seguida, você poderá executá-la clicando em um botão da Barra de Ferramentas de Acesso Rápido ou pressionando uma combinação de teclas. Isso dependerá de como você a configurar.*

Algumas formas de infecção e possíveis detecções/defesas são mostradas a seguir.

a) Execução de arquivos anexados a e-mails: o ideal é que por padrão o software utilizado para leitura de e-mails não abra um anexo automaticamente, e que o usuário tenha um software antivírus ativo quando da abertura/execução do arquivo;

b) Abertura de arquivos que possam conter macros (Word, Excel, etc.): ter certeza que quem criou o arquivo realmente criou macro(s), além de possuir um software antivírus ativo; se a utilização de macros não for necessária, recomenda-se desabilitá-los;

c) Abertura de arquivos armazenados em outros dispositivos (compartilhamento pela rede): recomendam-se os procedimentos citados nos dois itens anteriores;

d) Instalação de softwares de procedência duvidosa ou desconhecida: procurar uma fonte confiável e, após baixá-lo, verificar com mais de um software antivírus antes de executá-lo;

e) Ter alguma mídia removível infectada por vírus quando ele é ligado: o ideal é não permitir essa situação quando se tratar de uma mídia desconhecida, pois ela pode ter um sistema de inicialização, que além de carregar o sistema operacional, poderá infectar mídias internas do computador.

É importante deixar claro que apenas instalar software(s) antimalware não é o suficiente. A base de assinatura de malwares deve ser constantemente atualizada, pois novas pragas são criadas diariamente. Quanto mais softwares antimalware instalados, atualizados e em execução, mais seguro pode estar um computador, porém o desempenho será afetado. Aí depende da prioridade: desempenho x segurança.

Cavalo de Tróia (*Trojan Horse*)

Esse malware é fácil de associar seu comportamento com o nome. A Guerra entre troianos e gregos traz uma curiosidade: o cavalo de Tróia, documentado por alguns historiadores e considerado mito por outros. Trata-se de um cavalo de madeira grande dado pelos gregos aos troianos (daí surge também a expressão *presente de grego*).

Os troianos teriam colocado o cavalo dentro das muralhas que cercavam a cidade. À noite, soldados que estavam escondidos no interior do cavalo saíram, dominaram a cidade e abriram os portões para que o exército grego entrasse.

Ok, para que saber dessa estória toda? Simples, o malware que leva esse nome possui o mesmo comportamento, ou seja, é um software que além de desempenhar as funções previstas (ex.: jogo, proteção de tela, etc.), executa também outras atividades sem que o usuário tenha conhecimento. Imagine um jogo de corrida de carros que funciona perfeitamente, mas toda vez que é executado, também instala e configura um *backdoor*, além de avisar o criminoso que a máquina está ativa e pode ser acessada através de um determinado endereço IP e determinada porta.

Algumas funções que podem ser executadas por um *trojan* são:

a) Instalação de *keyloggers*, *backdoor* ou algum outro tipo de *malware*;

b) Cópia e envio de informações sensíveis, como senhas, números de cartões de crédito e dados pessoais;

c) Manipulação ou destruição de arquivos.

Uma forma de prevenção contra esse tipo de *malware* é o mesmo já abordado anteriormente, a utilização de softwares *antimalwares* atualizados, além de desconfiar de qualquer tipo de mensagem que envie em anexo algum software "magnífico", "espetacular"... 😊

Spyware e *Adware*

Essa categoria trata de softwares espiões (***spyware***), que podem ter uso legítimo (monitoramento de computadores de uma empresa ou de seu filho menor de idade) ou ilegítimo (instalado em um dispositivo sem o consentimento do proprietário/usuário). O software pode ser configurado para capturar apenas algumas atividades, afinal o criminoso quer receber apenas o que é útil para o seu "trabalho" de análise sobre os dados recebidos.

O ***adware*** (*advertisement software*) pode ser considerado uma subcategoria de *spyware*, mostrando propagandas ao usuário de acordo com seus hábitos. Digamos que você acesse sítios relacionados à computação forense, incluindo este curso que está lendo. Um *adware* poderia verificar esse hábito e direcionar propagandas de um curso russo sobre o tema! Não me pergunte o porquê de ser um curso russo...

O ***adware* pode ser legítimo** quando, por exemplo, o usuário concorda em utilizar um determinado *software* ou serviço. Você já leu algum termo de uso quando criou uma conta no Hotmail, Gmail, Facebook, etc.? Aposto que não! Pois é, muita gente não lê e clica logo em **"Concordo"**, permitindo que o serviço monitore seus hábitos e mostra propaganda de acordo com eles.

Keylogger

Muitas pessoas que acessam suas contas de redes sociais, e-mail, serviços bancários, além de outros serviços que solicitam senhas ou outros dados sensíveis, pensam que o simples fato de utilizar uma conexão criptografada (utilizando HTTPS, por exemplo) torna a atividade totalmente segura.

De fato, um protocolo com criptografia garante a confidencialidade dos dados, mas apenas os que estão "em trânsito", aqueles que estão trafegando pelos cabos ou pelo ar, incluindo sua senha!

O problema é o momento anterior ao envio dos dados, quando você informa seus dados via teclado, mouse, câmera ou qualquer dispositivo de entrada. Um ***Keylogger*** é capaz de **capturar as teclas pressionadas**, armazenando esses dados em um arquivo e enviando a quem tiver configurado o malware, via e-mail, FTP, ou outro meio.

Perceba que trata de uma subcategoria de *spyware*, pois trata-se de um espião de teclas! Mas, devido ao seu uso intenso por criminosos, esse tipo de malware ganhou mais notoriedade do que seu "pai".

Com a popularização dessa praga, sítios de bancos e de comércio eletrônico começaram a criar mecanismos para dificultar a captura de teclas. Surgiram teclados virtuais, utilização de *tokens*, utilização de assinatura digital, entre outros. Com relação aos teclados virtuais, as pragas evoluíram e começaram a capturar uma região da tela onde o clique do mouse era realizado, passando a se chamar ***screenlogger***.

Backdoor

Os *crackers* podem levar muito tempo para invadir um sistema e não querem ter o mesmo trabalho para retornar. Geralmente eles instalam um software que permite o acesso remoto através do uso de uma porta

TCP. Por exemplo, o *cracker* instala um software que utiliza a porta TCP 55555 e configura para que sempre que o dispositivo for inicializado, uma mensagem seja enviada a ele, comunicando qual o endereço IP está sendo usado.

Dessa forma, o *cracker* facilmente estabelece a comunicação através do endereço IP informado e a porta 55555, conforme o exemplo. O termo ***backdoor*** significa porta dos fundos, ou seja, aquela porta que o "dono da casa" não costuma observar e alguém consegue entrar sem ser convidado.

O *backdoor* também possibilita o uso legítimo, sendo muito utilizado para suporte técnico à distância, como por exemplo, o Teamviewer (https://www.teamviewer.com/pt/). Nesse caso, o usuário deve estar ciente que alguém acessará seu dispositivo para realizar as devidas configurações. Para isso, o ideal é que uma senha seja configurada para um único acesso, evitando que alguém descubra a senha e possa utilizar em outro momento, sem a devida autorização.

Worm

A principal característica de um *worm* é a capacidade de se **propagar automaticamente através de redes**, enviando cópias de si mesmo. Porém, diferentemente de um vírus, não embute cópias de si mesmo em outros softwares e **não necessita ser explicitamente executado** para se propagar.

Sua propagação ocorre através da **exploração de vulnerabilidades** existentes ou **falhas na configuração** de softwares instalados. Geralmente o *worm* tem como finalidade **consumir muitos recursos**, fazendo com que sistemas e redes tenham uma queda no desempenho ou até mesmo deixem de funcionar adequadamente. É aquele software que vem para incomodar, mesmo!

Algumas atividades promovidas por um *worm* são: geração de uma grande quantidade de pacotes na rede, criação de muitos arquivos no disco rígido com a intenção de utilizar todo ou a maior parte do espaço de armazenamento, criação de inúmeros processos que executem operações que consumam muito poder de processamento e memória RAM.

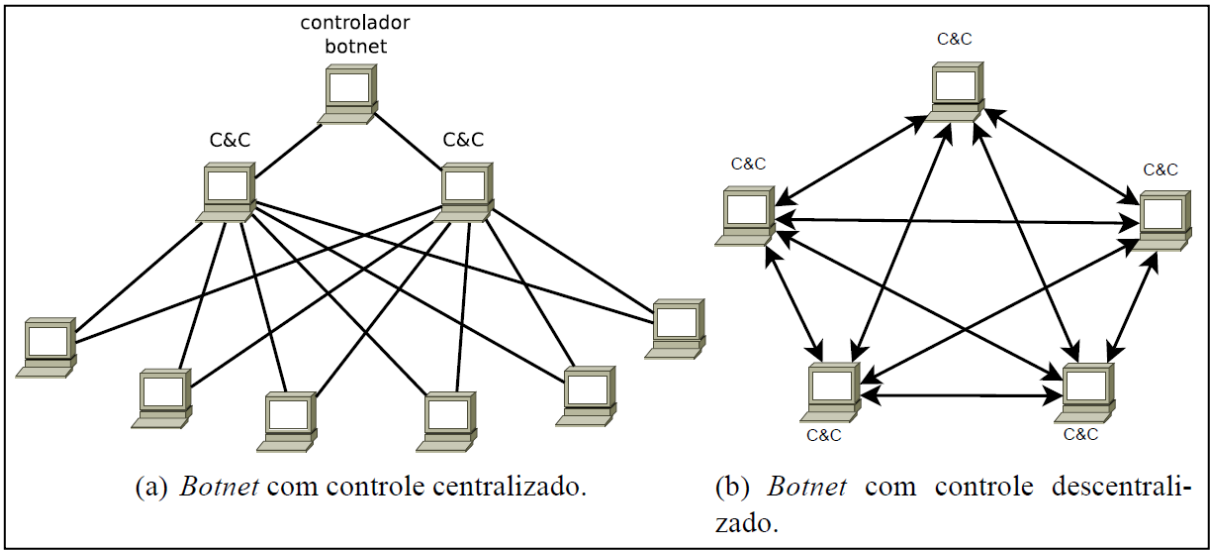
Bot e *Botnet*

O termo *bot* surgiu de *robot* (robô). Isso porque um robô é criado para obedecer a ordens se seres humanos (pelo menos por enquanto 😊), e essa categoria de malware faz isso mesmo! Um dispositivo infectado por um *bot* recebe comandos externos para realizar determinadas tarefas, como ataques DoS, *phishing*, etc.

O *bot*, também conhecido como zumbi, possui uma similaridade com o *worm*, a capacidade de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de softwares. O diferencial é que o *bot* possui mecanismos de comunicação com o invasor, permitindo o controle remoto. Geralmente é utilizado um servidor de IRC (*Internet Relay Chat*). Se você já usou um cliente IRC, isso denuncia sua idade...hoje o pessoal só quer utilizar redes sociais 😊

As ***botnets*** são redes formadas por *bots*. Essas redes muitas vezes são compostas por dezenas ou centenas de milhares de computadores infectados e ficam sob o comando de grupos de *crackers*, como o Anonymous. Um invasor que tenha controle sobre uma botnet pode utilizá-la para aumentar a potência de seus ataques e dificultar a investigação, visto que existiriam diversos endereços IP, em diversas regiões geográficas.

Uma botnet geralmente é descrita através de uma arquitetura centralizada, a qual possui um controlador apenas, mas existem também botnets que utilizam uma arquitetura descentralizada. Na figura abaixo são mostrados os dois cenários.



(a) *Botnet* com controle centralizado. (b) *Botnet* com controle descentralizado.

Figura retirada de uma dissertação de mestrado[1].

Obviamente que uma botnet com controle centralizado é mais simples de ser implementada, porém possui a desvantagem de ter um ponto único de falha. Basta inutilizar o controlador para que a botnet pare de funcionar. Uma botnet com controle descentralizado é o contrário, ou seja, mais difícil de ser implementada e mais robusta.

Uma notícia veiculada no sítio Tecmundo (https://www.tecmundo.com.br/spam/27868-veja-como-a-terceira-maior-botnet-do-mundo-foi-retirada-do-ar.htm) afirma que, em 2012, a *botnet* Grum era responsável por 18% das mensagens de spam que circulavam na Internet e tinha 120 mil endereços IP à disposição! Vale a pena ler essa matéria para entender como essa *botnet* surgiu e como terminou!

Rootkit

Após o êxito de uma invasão, o *cracker* procura utilizar mecanismos para destruir seus rastros e assegurar a sua presença no dispositivo comprometido, inclusive instalando softwares que facilitem seu retorno e permanência. O conjunto de softwares que fornece esses mecanismos é o *rootkit*.

Dentre as funcionalidades providas por softwares de um rootkit, destacam-se:

a) Softwares para esconder atividades e informações deixadas pelo invasor: arquivos, diretórios, processos, conexões de rede, etc.;

b) *Backdoors*, para facilitar o acesso futuro ao computador comprometido;

[1] "Arquitetura Distribuída e Automatizada para Mitigação de Botnet Baseada em Análise Dinâmica de Malwares", aluno: João Marcelo Ceron, UFRGS, 2010.

c) Softwares para exclusão de evidências em arquivos de *logs*;

d) *Sniffers*, para capturar pacotes na rede onde o computador está localizado, buscando informações sensíveis, como senhas;

e) *Scanners*, para procurar vulnerabilidades em outros computadores da rede;

Ransomware

Esse tipo de malware virou uma febre nos últimos anos. São aqueles malwares que criptografam arquivos e depois solicitam um resgate pela senha. O pagamento geralmente deve ser feito em *bitcoin* (ou outra criptomoeda), para dificultar o rastreamento. Os precursores dessas pragas virtuais, conhecidos como *scareware* (que ainda continuam ativos e podem ainda pegar "carona" nos *ransomwares*).

O objetivo do *scareware* (*scare* = assustar) é fazer com que a vítima pense que há algum problema no computador, quando na verdade não existe problema algum! O *ransomware*, ao contrário, realmente prejudica o computador, porque inutiliza o acesso aos arquivos por meio da criptografia. O *scareware* é mais "preguiçoso", apenas ameaça. A questão é que a mera ameaça muitas vezes já é eficaz, ou seja, não preciso um dano real. Então é comum que o tipo *scareware* pegue "carona" em outros golpes que ocorrem diariamente na web, incluindo o *ransomware*.

Fileless

Você poderá encontrar a expressão ***fileless malware*** ou ***fileless attack***. Como já teve questão sobre *fileless malware*, achei melhor colocar esse item dentro da aula de *malwares*.

Segundo a McAfee, esse tipo de malware surgiu em 2017 e, como o próprio nome sugere, não infecta nenhum arquivo e nem grava o próprio malware em disco. Então, como ele funciona? A figura abaixo ajuda a entender:

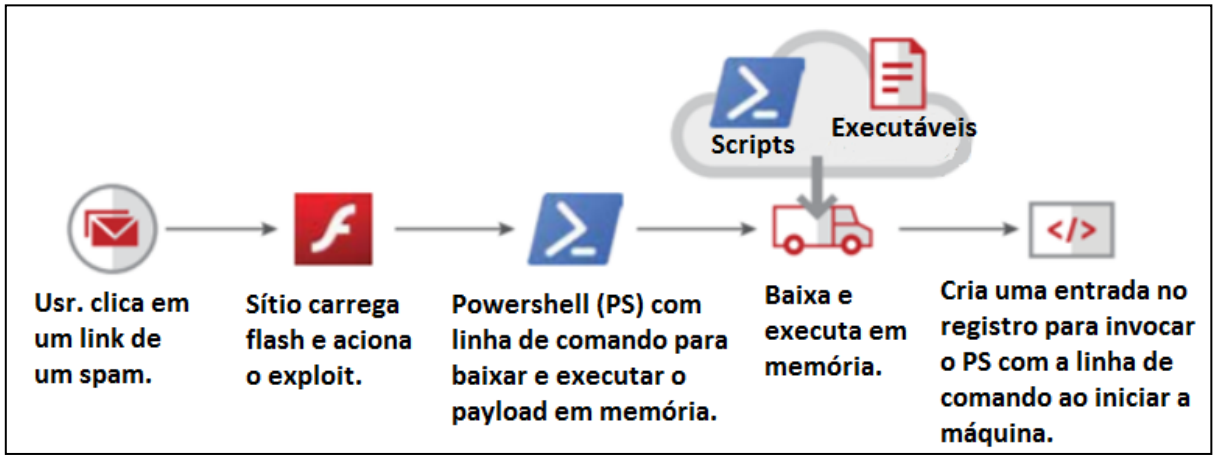


Figura traduzida de <https://www.mcafee.com/enterprise/pt-br/security-awareness/ransomware/what-is-fileless-malware.html>.

Como a figura mostrou, o malware é carregado em memória depois de algum link ter sido clicado pela vítima. Além disso, uma entrada no registro (geralmente) é criada para que o malware seja carregado

novamente ao se inicializar o computador. O malware não possui qualquer vínculo com o sistema de arquivos, pois nenhum arquivo é gravado.

8.2 – Questões Comentadas

63. (Quadrix/CRN-3ª Região - 2014) No que diz respeito à segurança da informação, leia as afirmativas e assinale a correta.

A) Botnet é um software que executa um ataque de negação de serviço.

B) Adware é um software que exibe conteúdo publicitário em seu computador, muitas vezes sem o consentimento do usuário.

C) DoS é um tipo de malware que monitora e captura o que é digitado em um computador.

D) Pharming é uma tentativa de envio de SPAM em massa que utiliza uma rede de computadores.

E) Phishing é uma forma de mascarar o endereço de um site, fazendo com que o endereço de um site falso se passe pelo endereço de um site legítimo.

Comentários:

(A) Até pode executar DoS, mas não apenas isso! **(B) Exatamente!** (C) Não e malware, é um ataque! (D) É aquele redirecionamento para um sítio falso; (E) Não é spam, é uma "pescaria" de vítimas.

64. (IADES/TER-PA - 2014) Programas maliciosos de computador podem colocar em risco a integridade dos sistemas que nele rodam e também podem proporcionar acesso indevido a informações sigilosas que ele contenha. Em sistemas Linux, é correto afirmar que os hackers costumam utilizar um software de invasão chamado

A) rootkit.

B) spyware.

C) vírus.

D) malware.

E) keylogger.

Comentários:

Na verdade, o rootkit possui uma coletânea de tipos de softwares de ataque, malwares, etc. Mas dentro das alternativas, o rootkit é a melhor opção, e não existe apenas no Linux. Logo, a **alternativa A** está correta e é o gabarito da questão.

65. (FGV/CGE-MA - 2014) A segurança na Internet constitui atualmente uma das preocupações dos administradores de redes, pelos danos que as pragas virtuais podem causar. Nesse contexto, analise as descrições a seguir.

I. São malwares que necessitam de uma interação do usuário para infectar uma máquina. O exemplo clássico é um anexo de e-mail contendo um código executável malicioso. Se o usuário receber e abrir tal anexo, o malware será executado na máquina.

II. São malwares capazes de entrar em uma máquina sem qualquer interação do usuário. O exemplo clássico é o de um usuário que está executando uma aplicação de rede frágil para o qual um atacante pode enviar um malware, que varre a Internet em busca de outros hospedeiros que estejam executando a mesma aplicação de rede vulnerável.

Essas descrições definem, respectivamente, os seguintes termos:

A) worm e sniffer.

B) vírus e worm.

C) proxy e vírus.

D) spyware e proxy.

E) sniffer e spyware.

Comentários:

I. Foco na necessidade de execução pelo usuário (abrir o anexo); II. Foco na autoexecução e a busca de vulnerabilidades na rede para se espalhar. Logo, a **alternativa B** está correta e é o gabarito da questão.

66. (IMA/Prefeitura de Canavieira-PI - 2015) É um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador:

A) Worm.

B) Firewall.

C) Sniffer.

D) Spyware.

Comentários:

Além de ter essa característica, o worm costuma consumir muitos recursos! Logo, a **alternativa A** está correta e é o gabarito da questão.

67. (FGV/DPE-MT - 2015) "Teclado Virtual" é uma técnica muito utilizada em aplicações via Internet que demandam maior segurança, como, por exemplo, entrada de senhas de banco ou cartões de crédito em transações bancárias. A ideia é que caracteres não sejam digitados pelo teclado físico e sim clicados com o auxílio do mouse em um teclado virtual que aparece na tela do computador. Seu principal objetivo é combater artefatos maliciosos conhecidos como

A) sniffers.

B) backdoors.

C) worms.

D) keyloggers.

E) rootkits.

Comentários:

Para evitar a captura por um keylogger, das teclas pressionadas, surgiram os teclados virtuais. Logo, a **alternativa D** está correta e é o gabarito da questão.

68. (IBFC/EBSERH - 2015) "Quando algum sistema operacional efetua um pedido de leitura de um arquivo, ele intercepta os dados que são requisitados e faz uma filtragem dessa informação, deixando o sistema ler apenas arquivos não infectados. Desta forma, o antivírus ou qualquer outra ferramenta ficam impossibilitados de encontrar o arquivo malicioso". Essa definição refere-se ao malware denominado:

A) exploit

B) rootkit

C) sniffer

D) quantum

E) adware

Comentários:

Quem gosta de esconder a lista de processos em execução, os nomes dos arquivos mostrados em um comando "ls", etc. é o rootkit, que consegue atuar em chamadas de sistema! Logo, a **alternativa B** está correta e é o gabarito da questão.

69. (CESPE/TCE-PA - 2016) Os bots, programas de computador que executam operações na forma de agentes em nome de um atacante, podem ser controlados remotamente e são capazes de, entre outras atividades, enviar spam.

Comentários:

Perfeito! Bot vem de “robot” e os robôs obedecem aos seres humanos (via comandos remotos), pelo menos por enquanto...questão **correta**!

70. (VUNESP/MPE-SP - 2016) Existem diversos tipos de malwares que podem infectar e prejudicar os computadores. O tipo de malware que se disfarça como programas legítimos para ser instalado nos computadores pelos usuários é denominado

A) Backdoor.

B) Hijacker.

C) Spyware.

D) Trojans.

E) Worms.

Comentários:

Lembre-se da estória do presente dos gregos aos troianos...o cavalo de Troia, que parecia ser apenas um cavalo, mas tinha uma surpresa dentro, tipo o Kinder Ovo 😊. Logo, a **alternativa D** está correta e é o gabarito da questão.

71. (FEPESE/Prefeitura de Lages-SC - 2016) Com relação à instalação e configuração de softwares de segurança, sobre ransomware, assinale a alternativa correta.

A) É um tipo de vírus que geralmente exclui ou troca de lugar (pasta) arquivos de usuário, como planilhas e documentos, do computador infectado.

B) É um tipo de malware ou vírus que geralmente criptografa os arquivos do computador infectado, impossibilitando sua abertura ou visualização.

C) É um tipo de malware ou vírus que realiza o monitoramento das atividades do computador infectado, com o objetivo de capturar senhas ou informações de cartões de crédito, por exemplo.

D) É um tipo de malware que instala um aplicativo no computador infectado com o objetivo de lançar ataques de negação de serviço a partir deste computador, dificultando a localização e rastreamento do agressor, e aumentando seu poder de processamento.

E) É um mecanismo de segurança e constitui uma resposta às tentativas de hackers e invasores de instalar malware no computador, reconhecendo e neutralizando esse tipo de ameaça digital.

Comentários:

Quando fala em malware que criptografa alguma coisa...99% de chance de ser ransomware 😊 A não ser que dê outros detalhes de outro tipo de malware. Logo, a **alternativa B** está correta e é o gabarito da questão.

72. (FCC/TER-PR - 2017) Um ataque massivo de hackers afetou empresas de diversos países do mundo. Até o momento, companhias de várias áreas de atuação, como comunicação, saúde e finanças foram prejudicadas. De acordo com informações da BBC, Estados Unidos, China, Rússia, Itália e Vietnã têm problemas similares com computadores 'sequestrados' por um tipo de vírus. Há ainda relatos de problemas na Espanha e Portugal.

Além de companhias como Vodafone, KPMG e Telefónica, o serviço de saúde britânico NHS também foi atingido por criminosos virtuais, de acordo com informações da agência Reuters. Ainda segundo a agência, o sistema de saúde do Reino Unido está respondendo aos ataques e, por conta dessa situação, diversos hospitais ao redor do país cancelaram consultas e atendimentos.

Os criminosos infectam as máquinas e demandam um resgate para 'liberar' os dados bloqueados. Alguns relatos informam que os malwares estão cobrando US$ 300 para liberar cada um dos computadores sequestrados e pedem o pagamento em bitcoins. Na rede social Twitter, vários usuários compartilharam imagens de suas telas de computadores após o sequestro. De acordo com relatos, o malware chega por e-mail e afeta, até então, apenas computadores com o sistema operacional Windows. (Adaptado de http://noticias.r7.com/tecnologia-e-ciencia/internet-sob-alerta-ataque-hacker-derruba-sistemas-de-empresas-em-todo-o-mundo-12052017)

Esse tipo de ataque é chamado

A) ransomware.

B) spoofing.

C) sniffing.

D) defacement.

E) DoS.

Comentários:

O texto é grande, mas se você passar o olho rapidamente já vê o pagamento de "US$ 300 para liberar cada um dos computadores sequestrados", o que já mata a questão! Logo, a **alternativa A** está correta e é o gabarito da questão.

73. (CONSULPLAN/TJ-MG - 2017) Códigos maliciosos (malwares) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. O programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim é conhecido como:

A) Backdoor.

B) Spyware.

C) Worm.

D) Rootkit.

Comentários:

Quando fala em retorno, pense em porta dos fundos (backdoor), afinal, o invasor não quer ser notado! Logo, a **alternativa A** está correta e é o gabarito da questão.

74. (FCC/TST - 2017) Um usuário notou que o computador ficou demasiadamente lento após a abertura de um e-mail recebido pela internet. Considerando esse sintoma de infecção e que colegas alegaram que receberam e-mails duvidosos desse usuário, trata-se de um malware do tipo

A) Backdoor.

B) Spyware.

C) Worm.

D) Rootkits.

E) Trojan.

Comentários:

Algumas palavras-chave: lento (consumo de muitos recursos), abertura de um e-mail e não disse que abriu o anexo (autoexecução). Com essas características, só pode ser worm! Logo, a **alternativa C** está correta e é o gabarito da questão.

75. (CESPE/ABIN - 2018) Uma das características das estruturas de comando e controle de malware descentralizadas é a garantia da existência de uma quantidade significativa de nós redundantes que devem ser atacados para que a rede de comando e controle associada ao malware seja desativada.

Comentários:

A questão fala em malware de forma genérica, mas possivelmente trata-se de uma botnet. Uma botnet com controle centralizado é mais simples de ser implementada, porém possui a desvantagem de ter um ponto único de falha. Basta inutilizar o controlador para que a botnet pare de funcionar. Uma botnet com controle descentralizado é o contrário, ou seja, mais difícil de ser implementada e mais robusta. Portanto, se houver N estruturas de comando e controle, para que a rede de comando e controle associada ao malware seja desativada todas as N estruturas de comando devem ser desativadas! Logo, a questão está **correta**.

76. (FCC/DPE-AM - 2018) O ataque do tipo Distributed Denial of Service - DDoS se utiliza de vários computadores conectados à rede para interromper os serviços da rede e dos equipamentos conectados a ela. Desta forma, para que ocorra um ataque DDoS é necessário que o atacante adquira o controle dos computadores tornando-os escravos, e para isso, utilizar um código malicioso do tipo

A) Spyware.

B) Botnet.

C) Adware.

D) Cavalo de Tróia.

E) Rootkit.

Comentários:

Os zumbis ou bots também podem ser chamados de escravos, formando uma botnet que recebe comandos de um criminoso, para efetuar atividades diversas, incluindo o ataque DDoS. Logo, a **alternativa B** está correta e é o gabarito da questão.

77. (CESPE/STJ - 2018) Fileless malware tem por principal característica a ocultação do endereço de entrada localizado no setor de início do ponto de montagem do sistema de arquivo do disco rígido.

Comentários:

O fileless malware não possui qualquer vínculo com o sistema de arquivos, pois nenhum arquivo é gravado! O que ocorre é o carregamento em memória e a sua execução, geralmente após um link ter sido clicado pela vítima. Para garantir futuras execuções, geralmente uma entrada é criada no registro para realizar novamente o procedimento descrito ao inicializar a máquina. Logo, a questão está **errada**.

78. (CESPE/STJ - 2018) Ransomware é um tipo de malware que cifra os arquivos armazenados no computador da vítima e solicita um resgate para decifrá-los.

Comentários:

Mais uma vez...como vimos na aula, geralmente só cobram isso sobre os ransomwares. Ou seja, são aqueles malwares que criptografam arquivos e depois solicitam um resgate pela senha. O pagamento geralmente deve ser feito em bitcoin (ou outra criptomoeda), para dificultar o rastreamento. Logo, a questão está **correta**.

79. (UFRR/UFRR - 2019) É um tipo de malware feito para extorquir dinheiro de sua vítima. Esse tipo de cyber ataque irá criptografar os arquivos do usuário e exigir um pagamento para que seja enviada a solução de descriptografia dos dados da vítima. O scareware é seu tipo mais comum e usa táticas ameaçadoras ou intimidadoras para induzir as vítimas a pagar. O texto acima se refere ao:

A) Spyware

B) Botnet

C) Spam

D) DDoS

E) Ransomware

Comentários:

Ransomware: esse tipo de malware virou uma febre nos últimos anos. São aqueles malwares que criptografam arquivos e depois solicitam um resgate pela senha. O pagamento geralmente deve ser feito em bitcoin (ou outra criptomoeda), para dificultar o rastreamento. Os precursores dessas pragas virtuais, conhecidos como *scareware* (que ainda continuam ativos e podem ainda pegar "carona" nos *ransomwares*).

O objetivo do *scareware* (scare = assustar) é fazer com que a vítima pense que há algum problema no computador, quando na verdade não existe problema algum! O *ransomware*, ao contrário, realmente prejudica o computador, porque inutiliza o acesso aos arquivos por meio da criptografia. O *scareware* é mais "preguiçoso", apenas ameaça. A questão é que a mera ameaça muitas vezes já é eficaz, ou seja, não preciso um dano real. Então é comum que o tipo *scareware* pegue "carona" em outros golpes que ocorrem diariamente na web, incluindo o *ransomware*.

Logo, a **alternativa E** está correta e é o gabarito da questão.

LISTA DE QUESTÕES

1. (FUNDATEC/IGP-RS - 2017) A Lei nº 12.737/2012, também conhecida como Lei dos Crimes Cibernéticos, dispõe sobre a tipificação criminal de delitos informáticos. O artigo 154-A dessa lei diz: "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa". A redação desse artigo mostra a intenção do legislador de tutelar valores protegidos constitucionalmente. Qual o bem jurídico protegido pelo artigo 154-A da Lei de Crimes Cibernéticos?

A) Segurança dos dados.

B) Dispositivos informáticos.

C) Rede de computadores.

D) Privacidade.

E) Livre acesso à informação.

2. (IBFC/Polícia Científica do Paraná - 2017) Assinale a alternativa correta, considerando o disposto expressamente na Lei nº 12.737, de 30/11/2012 (Lei dos crimes cibernéticos), sobre a pena aplicável a quem invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita?

A) Detenção de 1 (um) a 2 (dois) anos, e multa, aumentando-se a pena de um terço à metade se da invasão resultar prejuízo moral.

B) Detenção de 1 (um) a 2 (dois) anos, e multa, aumentando-se a pena de um sexto a um terço se da invasão resultar prejuízo econômico.

C) Detenção de 3 (três) meses a 1 (um) ano, e multa, aumentando-se a pena de um sexto a um terço se da invasão resultar prejuízo econômico.

D) Detenção de 3 (três) meses a 1 (um) ano, e multa, aumentando-se a pena de um terço à metade se da invasão resulta prejuízo moral.

E) Detenção de 6 (seis) meses a 2 (dois) anos, e multa, aumentando-se a pena de um sexto a um terço se da invasão resulta prejuízo moral.

3. (IBFC/Polícia Científica do Paraná - 2017) Assinale a alternativa correta, considerando o disposto expressamente na Lei no 12.737, de 30/11/2012 (Lei dos crimes cibernéticos), sobre a AÇÃO PENAL nos casos do crime praticado por quem invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter informações sem autorização expressa ou tácita do titular do dispositivo:

A) Nesses casos, somente se procede mediante representação, mesmo que o crime seja cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos

B) Nesses casos, procede-se independentemente de representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios.

C) Nesses casos, procede-se independentemente de representação, salvo se o crime é cometido contra empresas concessionárias de serviços públicos.

D) Nesses casos, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

E) Nesses casos, a ação penal é sempre pública e incondicionada.

4. (UFMT/IF-MT - 2015) Sobre a tipificação dos delitos informáticos segundo a Lei nº 12.737/2012, assinale a afirmativa correta:

A) Pratica crime de invasão de dispositivo informático aquele que, com autorização expressa do titular do dispositivo, instala vulnerabilidades para obter vantagem ilícita.

B) Pratica o crime de perturbação de serviço telemático, telefônico ou informático aquele que interrompe o serviço telemático, telefônico ou informático, salvo se cometido por ocasião de calamidade pública.

C) Pratica crime de invasão de dispositivo informático aquele que adultera ou destrói dados ou informações sem autorização expressa ou tácita do titular do dispositivo.

D) Pratica o crime de falsificação de documento público aquele que falsifica, no todo ou em parte, cartão de crédito ou de débito, obtendo ou não vantagem ilícita.

5. (SIGMA/Câmara Municipal de Carapicuíba-SP - 2013) Cinco meses após hackers roubarem e divulgarem na internet fotos íntimas da atriz Carolina Dieckmann, o Congresso Nacional aprovou proposta que tipifica crimes cibernéticos. Batizada de "Lei Carolina Dieckmann", a legislação que torna crime a invasão de computadores foi sancionada por Dilma Rousseff em dezembro de 2012. Essa lei é a Lei Nº:

A) 12.373.

B) 12.737.

C) 10.737.

D) 10.373.

6. (FUNDATEC/PGE-RS – 2010) Essa questão baseia-se na palestra intitulada "A Arte de Enganar", ministrada pelo ex-hacker e atual consultor de segurança Kevin Mitnick, durante o Campus Party 2010, que ocorreu em São Paulo, em janeiro desse ano. Nessa palestra, Mitnick abordou métodos usados por hackers para obter informações sigilosas. Segundo ele "Muitos ataques de hackers não necessitam de grande conhecimento técnico, mas sim de poder de convencimento para que a própria vítima forneça as informações desejadas". Mitnick admitiu que, muitas vezes, se valeu de truques de convencimento verbal e mentiras que o levaram a invadir diversos sistemas nos quinze anos em que se manteve nesta atividade. Na opinião de Mitnick, bastava persuadir funcionários mais desavisados a compartilharem informações vitais, como nomes de login e senhas; foi assim que ele afirma ter invadido a rede da empresa Sprint, se passando por um engenheiro da firma Nortel Networks para o qual os funcionários passaram dezenas de logins e senhas para o acesso aos switches. Nesse caso, a utilização da persuasão, dissimulação e mentiras verbais para convencer funcionários a compartilharem informações vitais, como nomes de login e senhas, para ter acesso não autorizado a diversos ativos de redes, como, por exemplo, switches, caracteriza-se por ser um método de ataque denominado

A) Hoax.

B) Spyware.

C) Adware.

D) Keyloggers.

E) Engenharia Social.

7. (CESPE/Polícia Federal – 2013) O ser humano possui traços psicológicos e comportamentais que o tornam vulneráveis a ataques de engenharia social, como a vontade de ser útil, a busca por novas amizades, esteganografia e autoconfiança.

8. (IBFC/PC-RJ – 2013) Existe um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. Estamos falando do método de:

A) Colarinho Branco.

B) Engenharia de Serviço.

C) Criptografia Privada.

D) Engenharia Social

E) Sociologia criptográfica.

9. (UESPI/PC-PI – 2014) A utilização de práticas para obter acesso a informações sigilosas em organizações e sistemas computacionais, por meio da exploração de confiança das pessoas com habilidades de persuasão, é chamada de

A) engenharia reversa.

B) spyware.

C) engenharia social.

D) worm.

E) botnet.

10. (INSTITUTO CIDADES/CONFERE – 2016) São objetivos da engenharia social, EXCETO

A) Técnica para prevenir ataques aos ativos.

B) Espionagem industrial.

C) Obter informações privilegiadas para ter vantagem.

D) Roubo de senhas de bancos ou cartões de crédito.

11. (FCC/TRT-24ª Região – 2017) Um Técnico de Informática, ao acessar o site da organização para a qual trabalha, encontrou-o totalmente desfigurado, com o conteúdo das páginas alterado. Ao buscar razões para este tipo de ataque que viola a segurança das informações, verificou que um atacante, para desfigurar uma página web, pode:

– explorar erros da aplicação web;

– explorar vulnerabilidades do servidor de aplicação web;

– explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação web;

– invadir o servidor onde a aplicação web está hospedada e alterar diretamente os arquivos que compõem o site;

– furtar senhas de acesso à interface web usada para administração remota.

O Técnico concluiu, corretamente, que este tipo de ataque é conhecido como

A) inundação UDP.

B) engenharia social.

C) wardriving

D) IP spoofing.

E) Defacement

12. (FUNDATEC/IGP-RS – 2017) O conceito de Segurança da Informação (SI) pode ser definido simplesmente como o conjunto de medidas que possuem o objetivo de tornar as informações seguras, sendo a cultura dos usuários um dos alicerces da segurança da informação mais sensíveis. Qual é a técnica utilizada pelos criminosos que explora diretamente a cultura dos usuários?

A) Esteganografia.

B) Criptografia.

C) Autenticidade.

D) Confidencialidade.

E) Engenharia social.

13. (IESES/IGP-SC – 2017) Considerando as práticas do que se denomina 'Engenharia Social' no contexto da Segurança da Informação, é correto afirmar que:

A) Um 'ataque' de engenharia social pode utilizar estratégias de relacionamento pessoal para obtenção de informações sigilosas.

B) A utilização de certificados digitais A3 é mais adequada que certificados A1.

C) Algoritmos de 'força bruta' são um instrumento comumente utilizados para descoberta de informações.

D) A instalação de softwares detectores de 'phishing' é uma estratégia para evitar ataques de um engenheiro social.

14. (FCC/TRT-9ª Região – 2013) É um tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social, ocorre por meio do envio de mensagens eletrônicas que

- tentam se passar pela comunicação oficial de uma instituição conhecida, tal como banco, empresa ou site popular;

- procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;

- informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;

- tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas web.

Este meio de ataque é conhecido como

A) trojan.

B) phishing.

C) malware.

D) sniffing.

E) spoofing.

15. (FGV/SUDENE-PE – 2013) Um usuário acessa sua caixa de mensagens e abre uma mensagem supostamente enviada pelo seu banco solicitando que ele acesse o site do banco e atualize alguns dados. O usuário clica no link e um site idêntico ao do banco aparece. Ele entra com a sua senha, atualiza os dados e os transmite. Depois de algum tempo, ele percebe que foi enganado, pois uma grande quantia foi retirada da sua conta. Assinale a alternativa que indica o tipo de ataque que ele sofreu.

A) DDoS.

B) phreaking.

C) DoS.

D) phishing.

E) adware.

Comentários:

A clássica “isca” que foi fisgada! Está claro que a resposta é phishing. E as outras, por que estão erradas? DoS e DDoS são ataques de negação de serviço. Phreaking é a atividade de cracking aplicado à telefonia. Adware

é um malware que mostra propagandas (veremos adiante). Logo, a **alternativa D** está correta e é o gabarito da questão.

16. (FGV/DPE-RO – 2015) Para tentar diminuir as possibilidades do ataque phishing deve-se:

A) realizar a leitura de e-mail através de sites web, pois o e-mail não é trazido para a máquina do cliente;

B) configurar adequadamente um filtro para pacotes ICMP no servidor de correio;

C) usar o serviço NFS no cliente de e-mail;

D) implantar filtros para mensagens spam ou em "black-list";

E) realizar leitura de e-mail através do protocolo pop ou imap com ssl, usando criptografia na rede.

17. (FCC/ELETROBRAS-ELETROSUL - 2016) Considere, por hipótese, que a Eletrosul deseja aumentar a segurança das informações utilizando registros das atividades de seus colaboradores. A partir da análise destes registros armazenados em arquivo ou em base de dados, a empresa pode ser capaz de:

- detectar o uso indevido de computadores, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema;

- detectar um ataque, como de força bruta, ou a exploração de alguma vulnerabilidade;

- rastrear ou auditar as ações executadas por um usuário no seu computador, como programas utilizados, comandos executados e tempo de uso do sistema;

- detectar problemas de hardware ou nos programas e serviços instalados no computador.

Estes registros são denominados

A) backups.

B) phishing.

C) logs.

D) hashes.

E) firewalls.

18. (CESPE/TCE-PA – 2016) Diferentemente dos golpes de phishing, os ataques de spear phishing são realizados mediante o envio aleatório e em massa de emails enganosos para múltiplos usuários, para a obtenção de informações bancárias das vítimas ou apropriação da identidade delas.

19. (FCC/Prefeitura de Teresina-PI – 2016) O usuário de um computador instalado na rede local de computadores - LAN gerenciada pelo Analista de Suporte informou e questionou sobre o recebimento de uma mensagem de e-mail que solicitava a atualização das suas informações de usuário na LAN. Identificando que se tratava de uma mensagem falsa, o Analista concluiu que se tratava de um ataque do tipo.

A) DoS.

B) Spoofing.

C) Flooding.

D) Spam.

E) Phishing.

20. (COSEAC/Prefeitura de Maricá-RJ – 2018) Na segurança da Informação existe um tipo de ataque em que iscas como "mensagens não solicitadas" são utilizadas para capturar senhas e dados de usuários na Internet. Esse ataque é conhecido como:

A) spoofing.

B) hijacking.

C) engenharia social.

D) phishing.

E) cookies.

21. (FGV/AL-RO – 2018) O tipo de ataque na Internet em que pessoas comuns são contatadas por e-mail, com mensagens que parecem genuínas, contendo nomes e informações que fazem referência a empresas conhecidas, como bancos, porém, contendo links disfarçados para arquivos maliciosos, é denominado

A) Spoofing.

B) DoS.

C) DDoS.

D) Phishing.

E) Bluebugging.

22. **(CESPE/TER-RJ - 2012) Pharming é um tipo de golpe em que há o furto de identidade do usuário e o golpista tenta se passar por outra pessoa, assumindo uma falsa identidade roubada, com o objetivo de obter vantagens indevidas. Para evitar que isso aconteça, é recomendada a utilização de firewall, especificamente, o do tipo personal firewall.**

23. **(FUNDEP/IPSEMG - 2013) Analise as seguintes afirmativas acerca de golpes/fraudes na Internet. Em seguida, assinale com V as verdadeiras e com F as falsas.**

( ) O pharming é um tipo de golpe que redireciona um usuário para um site falso.

( ) O phishing é um tipo de fraude em que o adversário se utiliza da combinação de meios técnicos e engenharia social para lograr sucesso.

( ) O furto de identidade é quando o adversário tenta se passar por um usuário, em geral, legítimo.

( ) O boato (hoax) é um tipo de golpe em que engenharia social é utilizada eminentemente para invadir computadores alheios.

Assinale a alternativa que apresenta a sequência CORRETA.

A) V V V F.

B) V V F F.

C) F V V F.

D) V F F V.

24. **(CESPE/TJ-SE - 2014) Um tipo específico de phishing, técnica utilizada para obter informações pessoais ou financeiras de usuários da Internet, como nome completo, CPF, número de cartão de crédito e senhas, é o pharming, que redireciona a navegação do usuário para sítios falsos, por meio da técnica DNS cache poisoning.**

25. **(Quadrix/CRN-3ª Região - 2014) Leia atentamente a seguinte definição.**

"Uma tentativa de defraudar os internautas sequestrando o nome do domínio do site ou URL e redirecionando os usuários a um site impostor, no qual são feitas solicitações fraudulentas de informações."

A definição acima refere-se a:

A) Phishing.

B) SPAM.

C) Web Bot.

D) Pharming.

E) Engenharia social.

26. (FCC/TCE-GO - 2014) Ao tentar entrar em alguns sites de comércio eletrônico para comprar produtos de seu interesse, Maria percebeu que estava sendo redirecionada para sites muito semelhantes aos verdadeiros, mas que não ofereciam conexão segura, nem certificado digital. Pela característica do problema, é mais provável que Maria esteja sendo vítima de

A) vírus.

B) worm.

C) trojan.

D) backdoor.

E) pharming.

27. (OBJETIVA/Prefeitura de Cidreira-RS - 2016) É um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Nesse caso, quando o usuário tenta acessar um site legítimo, o seu navegador web é redirecionado, de forma transparente, para uma página falsa. Essa forma de phishing é conhecida como:

A) Boot.

B) EdoRam.

C) Bios.

D) Pharming.

28. (IFSul-MG/IFSul-MG - 2016) De acordo com o CERT.br: "(...) é uma técnica que consiste em alterar campos do cabeçalho de um email, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.". Considerando um servidor de e-mails configurado erradamente e que um usuário mal-intencionado teve acesso a este servidor para o envio de mensagens com origem forjada, qual foi a técnica utilizada para o envio dessas mensagens?

A) Pharming.

B) Spoofing.

C) Phishing.

D) Spam.

29. (FCC/TRF-3ª Região - 2016) Para responder a questão considere as informações abaixo.

Os Técnicos Judiciário de TI de um Tribunal têm ciência sobre ataques da internet e por isso adotam medidas de defesa contra (I) falsificação de e-mail porque esta técnica consiste em alterar (II) elementos do e-mail de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. O que possibilita esta técnica de falsificação é a característica de um (III) protocolo de Internet que permite que campos do From, do Reply to e do Return-Path sejam adulterados. Isto é bastante usado por alguns hackers para propagação de códigos maliciosos, envio de spam e (IV) tipos de ataques que atuam informando, falsamente, que a não execução dos procedimentos descritos pode acarretar sérias consequências, como, por exemplo, a inscrição em serviços de proteção de crédito e coisas semelhantes.

O nome pelo qual a falsificação referida em I é conhecido e os elementos do e-mail alterados referidos em II correspondem, correta e respectivamente, a e-mail

A) pharming e texto da mensagem.

B) splashing e dados do remetente.

C) spoofing e campos do cabeçalho.

D) brut force e dados do destinatário.

E) defacement e campos do cabeçalho.

30. (FUNDATEC/IGP-RS - 2017) Peritos criminais da Seção de Computação Forense foram designados para realizar exame na rede de computadores de uma empresa que estaria sendo alvo de crimes cibernéticos. Enquanto estava ocorrendo o suposto ataque, os peritos criminais coletaram o tráfego de rede do local examinado. Nesses vestígios coletados, os peritos criminais identificaram pacotes que eram direcionados para um DNS que não era de uma autoridade real; sempre que os usuários tentavam acessar a página na internet de um determinado banco, eram redirecionados para uma página de escolha do criminoso. Analisando o servidor de DNS, os peritos constataram que foi adicionado um registro de DNS falso no cache do servidor de DNS que redirecionava os usuários para sites falsos. Com base nos fundamentos de investigação em redes de computadores, assinale a alternativa que explica o redirecionamento de DNS e a provável técnica utilizada pelos criminosos.

A) Os criminosos usaram a técnica de envenenamento de DNS ou DNS Poisoning.

B) A técnica utilizada pelos criminosos é conhecida como DNS oculto ou DNS redirection.

C) Este é um caso clássico em que o criminoso utilizou de injeção de SQL ou SQL injection.

D) Os vestígios coletados pelos peritos criminais apontam para uma técnica conhecida como roubo de sessão ou DNS session injection.

E) O registro de DNS falso no cache do servidor indica que os criminosos utilizaram um ataque de negação de serviço ou Denial of Service (DoS), que fez com que todos os usuários que tentavam acessar a internet fossem redirecionados para um servidor de DNS do criminoso.

31. (UFMT/UFSBA - 2017) Phishing é o tipo de fraude na internet, por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social. Sobre esse assunto, analise as afirmativas.

I - Pharming é um tipo específico de phishing que envolve o redirecionamento da navegação do usuário para sites falsos, de forma que, quando ele tenta acessar um site legítimo, o navegador Web é redirecionado para uma página falsa.

II - Por se tratar de uma fraude pouco comum e, na maioria das vezes, inofensiva, descarta-se a utilização de mecanismos de segurança, como programas antimalware, firewall pessoal e filtros antiphishing.

III - Sites de comércio eletrônico ou Internet Banking confiáveis, na maioria das vezes, utilizam conexões seguras, por exemplo HTTPS, quando dados sensíveis são solicitados.

IV - O phishing pode ocorrer por meio do envio de mensagens eletrônicas que tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular.

Estão corretas as afirmativas.

A) I e IV, apenas.

B) II e III, apenas.

C) II, III e IV, apenas.

D) I, III e IV, apenas.

32. (CESPE/Polícia Federal - 2018) Um tipo de ataque contra o serviço DNS é o pharming, que envolve o redirecionamento do navegador do usuário para sítios falsos por meio da técnica conhecida como envenenamento de cache DNS.

33. (UNEMAT/UNEMAT - 2018) Pharming é uma ameaça de segurança do tipo phishing, que tem o intuito de direcionar o usuário para sites falsos, por meio de alterações no servidor de DNS.

Cartilha de Segurança para Internet, versão 6.0 / CERT.br - São Paulo: Comitê Gestor da Internet no Brasil, 2017.

Considerando este tipo de ataque, analise as asserções a seguir e a relação entre elas.

I. Usuários que informam o endereço URI (Universal Resource Identifier) na barra do navegador evitam ataques do tipo Pharming.

II. Usuários que informam o endereço URL (Universal Resource Locator) na barra do navegador evitam ataques do tipo Pharming.

III. Visando mitigar ameaça do tipo Pharming, o administrador de redes deve instruir o usuário a inspecionar se o certificado se segurança é valido e corresponde a instituição proprietária do site, quando utilizado o protocolo HTTPS.

IV. Quando o usuário acessa o endereço legítimo de um site em seu navegador web, sua requisição será redirecionada, de maneira transparente, para uma página falsa.

Sobre o exposto assinale a alternativa que apresenta as afirmações corretas.

A) I e II.

B) II e III.

C) I e IV.

D) II e IV.

E) III e IV.

34. (CESPE/Polícia Federal - 2004) A captura de pacotes que trafegam na rede com uso de um sniffer é um exemplo de ataque para o qual não há nenhuma forma de detecção possível pelo administrador de rede.

35. (CESPE/TJ-AL - 2012) As técnicas que realizam a detecção remota de sniffers na rede sem acessar cada equipamento do segmento de rede são

A) coordinated scans e DNS detection.

B) MAC detection e load detection.

C) DNS detection e dumpster diving.

D) decoy e MAC intrusion.

E) fail detection e load detection.

36. (AOCP/TCE-PA - 2012) Servidores conectados à Internet estão sujeitos a vários tipos de ataques. São alguns desses tipos de ataques, apenas:

A) DoS, flood, trojan.

B) vírus, trojan e adware.

C) backdoor, waf, sniffer.

D) phishing, flood, spoofing.

E) vírus, sniffer, keylogger.

37. (FCC/TRT-5ª Região - 2013) Há diversas técnicas e práticas utilizadas para monitoramento e análise de tráfego de dados nas redes. Considere:

I. É uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos. Pode ser utilizada por administradores de redes, de forma legítima, para detectar problemas, analisar desempenho e monitorar atividades maliciosas ou por atacantes, de forma maliciosa, para capturar informações como senhas, números de cartão de crédito e conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

II. Prática que pode ser utilizada por provedores de acesso à internet com o objetivo de limitar o tamanho da banda para os protocolos e programas que usam mais a rede, notadamente os de transferência de arquivos grandes, como P2P. Alguns provedores limitam, inclusive, a transmissão de arquivos via FTP. Esta prática é realizada para garantir que os usuários, que não utilizam esses protocolos de transferência ou não fazem downloads de grandes arquivos, possam ter acesso a outros tipos de serviço sem enfrentar lentidão na rede, embora seja condenada por algumas instituições protetoras dos direitos do consumidor.

As descrições I e II referem-se, respectivamente, a

A) IDS e NAT.

B) traffic shaping e sniffer.

C) NAT e VoIP.

D) sniffing e traffic shaping.

E) IDS e Torrent.

38. (CESPE/MS - 2013) O sniffer, que pode ser do tipo filtro de pacotes e do tipo proxy de aplicações, é um dispositivo que tem por objetivo aplicar uma política de segurança a determinado ponto de uma rede de computadores.

39. (Quadrix/CRO-GO - 2013) Como é chamado o software capaz de interceptar e registrar o tráfego de dados em uma rede de computadores?

A) Vírus

B) Trojan.

C) Sniffer.

D) Worm.

E) Spyware.

40. (FCC/TJ-AP - 2014) Um especialista em segurança de redes desconfia que uma aplicação está sendo muito utilizada e está diminuindo a capacidade dos recursos de rede. Para comprovar suas suspeitas resolveu utilizar um sniffer de rede muito popular que pode ser utilizado em redes Unix e Windows para analisar os pacotes recebidos e transmitidos por qualquer interface de rede, sendo possível aplicar vários tipos filtros. Este sniffer é conhecido como

A) Asterisk.

B) Vyatta.

C) Everest.

D) Wireshark.

E) NDISwrapper.

41. (CESPE/Telebras - 2015) Sniffers são programas aparentemente inofensivos cuja principal característica é utilizar a técnica de mascaramento. A técnica em questão permite, por exemplo, que um sniffer seja anexado a um jogo, que, por sua vez, ao ser instalado em um computador, coletará informações bancárias do usuário.

42. (FGV/CODEBA - 2016) No contexto do correio eletrônico, muitas vezes um tipo de mensagem chega ao usuário sem que ele tenha solicitado ou considerado a hipótese de recebê-la. Essas mensagens são transmitidas e inseridas com finalidade comercial, tentando fazer com que a pessoa adquira algum produto ou serviço. Essas mensagens são conhecidas por

A) swap.

B) sniffer.

C) scrum.

D) spoof.

E) spam.

43. (FCC/TRF-3ª Região - 2016) Um usuário que se conecta em uma rede wifi em um local público, por exemplo, está exposto a vários tipos de ataques Man in The Middle – MITM. Nesse sentido, para tomarem alguma ação preventiva, os Técnicos Judiciários de TI do TRF3 devem estar atentos a um desses tipos de ataque, o Session Hijacking, que é utilizado para o sequestro de sessão por meio de

A) modificação do channel Cain & Abe

B) roubo de cookie que utiliza HTTP.

C) envenenamento do cache HTTP.

D) interceptação do tráfego da rede para capturar uma consulta DNS.

E) sequestro do ettercap, via sniffer.

44. (IBFC/EBSERH - 2016) Para o gerenciamento de rede, monitoramento e diagnóstico de ambientes computacionais, muitas vezes, utiliza-se uma ferramenta, constituída de um software ou hardware, que é capaz de interceptar e registrar o tráfego de dados em uma rede de computadores denominado tecnicamente de:

A) jitter

B) sniffer

C) ping

D) gateway

E) noise

45. (FCC/TRF-5ª Região - 2017) Os Sniffers de rede podem ser ferramentas adequadas para monitorar o tráfego da rede local. Para aumentar a eficiência do Sniffer deve-se utilizá-lo no modo promíscuo em que

A) apenas os pacotes endereçados para um servidor são monitorados.

B) pacotes criptografados são decifrados e analisados.

C) pacotes são gerados aleatoriamente para analisar a correta configuração do switch.

D) todos os pacotes que trafegam pela rede local são monitorados.

E) responde automaticamente a todos os pacotes de verificação de estado da rede.

46. (UPENET/IAUPE/UPE - 2017) Uma das ferramentas mais poderosas para gerenciar o funcionamento de uma rede de computadores é um sniffer. Qual dos abaixo é um sniffer?

A) Traceroute

B) Wireshark

C) Ping

D) Netstat

E) SystemMonitor

47. (UFU-MG/UFU-MG - 2018) Em um equipamento rodando Linux, o comando tcpdump é um dos mais, se não o mais, "famoso" sniffer para sistemas GNU/Linux. Com ele, podemos realizar análises e solucionar problemas. O comando tcpdump permite aos administradores a capacidade de monitorar

A) desempenho do servidor.

B) desempenho da aplicação.

C) tráfego e atividade da rede.

D) arquivos e diretórios.

48. (FGV/Banestes - 2018) Com relação ao uso de sniffers, analise as afirmativas a seguir:

I. Um sniffer costuma ser utilizado para encontrar outros sniffers presentes em outras máquinas na rede.

II. Podem ser utilizados como fonte de negação de serviço na sub-rede onde operam.

III. A interface de rede deve estar operando em modo promíscuo para que um sniffer funcione adequadamente.

Está correto somente o que se afirma em:

A) I;

B) II;

C) III;

D) I e II;

E) II e III.

49. (CESPE/Polícia Federal - 2018) Um dos objetivos do firewall é monitorar todo o tráfego de dados entrando e saindo de uma rede local e entrar em ação ao identificar um sniffer externo.

Comentários:

Um sniffer atua de forma passiva, apenas capturando pacotes de dados, sem transmiti-los. Logo, um firewall não poderia detectar um sniffer. Logo, a questão está **errada**.

50. (FGV/AL-BA - 2014) Considere que um hacker comprometa milhares de hosts ao redor do mundo, criando uma botnet com intenção maliciosa. Em determinada ocasião, comandados por um computador mestre, estes hosts executam um ataque conjunto a um determinado servidor web ou DNS, consumindo a largura de banda do servidor e comprometendo seu funcionamento. O cenário descrito é típico de um ataque denominado

A) worms.

B) spoofing.

C) phishing.

D) DDoS

E) DoS.

51. (CESPE/MEC - 2015) No que se refere aos ataques de negação de serviço, julgue o item que se segue. Nesse sentido, considere que a sigla DDoS, sempre que utilizada, se refere ao ataque Distributed Denial of Service.

Ataques Xmas-DDoS (christmas tree packets) são caracterizados pela inundação de pacotes ICMP tipo 8 em uma rede de dados.

52. (CESPE/MEC - 2015) Ataques refletivos de DDoS de NTP têm como objetivo indisponibilizar os serviços de NTP pelo mundo, atrasando-os em uma hora, o que gera inconsistências nos horários registrados pelos logs e nas trocas de mensagens.

53. (FCC/TRT-3ª Região - 2015) O Administrador de uma rede local de computadores, que utiliza IPs Classe B, identificou que o servidor da rede local recebeu requisições de acesso de um computador da mesma rede local com IP: 192.168.1.1. O tipo de ataque identificado é conhecido como

A) DoS.

B) Spoofing.

C) Scanning.

D) Defacement.

E) DDoS.

54. (VUNESP/TCE-SP - 2015) Existem diferentes tipos de ataques de hackers por meio das redes de computadores. Nesse contexto, o ataque no qual vários computadores realizam requisições ou enviam pacotes malformados para um sistema pela rede é denominado

A) DoS.

B) DDoS.

C) Flooding.

D) Phishing.

E) Spoofing.

55. (IDIB/Prefeitura de Limoeiro do Norte-CE - 2016) São ameaças de Internet, EXCETO

A) Malware.

B) Criptografia.

C) DdoS.

D) Negação de Serviço.

56. (CESPE/TRT-7ª Região - 2017) O ataque que amplia o número de acessos a um servidor, gerando indisponibilidade de recursos aos usuários, é denominado

A) phishing.

B) DoS.

C) spoofing.

D) adware.

57. (FCC/Prefeitura de Teresina-PI - 2016) Trata-se de um tipo de ataque em redes de computadores que compreende a ação de um Botnet que concede o controle de vários computadores para enviar constantemente pacotes de dados a um determinado servidor. O tipo de ataque descrito é

A) Spoofing.

B) DDoS.

C) Phishing.

D) DoS.

E) Spam.

58. (CESGRANRIO/UNIRIO - 2016) Um ataque de DDoS (Distributed Denial of Service) visa a consumir os recursos do alvo em larga escala para provocar uma sobrecarga que prejudique o fornecimento do serviço. Quando esse ataque é classificado como DDoS refletor, os zumbis escravos geram pacotes, com uma solicitação de resposta, que

A) são destinados aos próprios zumbis escravos para amplificar o ataque ao alvo.

B) são destinados aos zumbis mestres que, por sua vez, os repassam para o alvo.

C) possuem seus próprios endereços no campo de origem dos pacotes.

D) possuem o endereço do alvo no campo de origem dos pacotes.

E) possuem os endereços dos zumbis mestres no campo de origem dos pacotes.

59. (FCC/DPE-RS - 2017) O tipo de ataque DDoS - Distributed Denial of Service que explora a vulnerabilidade do processo de comunicação do protocolo TCP é o

A) SYN Flood.

B) NTP Flood.

C) Ping of Death.

D) UDP Flood.

E) VoIP Flood.

60. (IBFC/Polícia Científica-PR - 2017) O "ping da morte" (ping of death) é um ataque que objetiva a indisponibilidade de servidores por meio do envio maciço de pacotes de ping malformados. Um ataque dessa categoria é classificado como:

A) Worm

B) Ransomware

C) Backdoor

D) Spyware

E) DoS/DDoS

61. (CESPE/ABIN - 2018) Os testes CAPTCHA são eficientes contra os ataques DDoS volumétricos e os de exaustão das conexões TCP, mas são inócuos contra os ataques DDoS de camada de aplicação.

62. (CESPE/FUB - 2018) O principal objetivo de um ataque DDoS é causar superaquecimento e danos físicos ao hardware do processador da máquina-alvo, por meio do envio simultâneo de um volume muito grande de requisições de conexão a partir de milhares de máquinas distribuídas.

63. (Quadrix/CRN-3ª Região - 2014) No que diz respeito à segurança da informação, leia as afirmativas e assinale a correta.

A) Botnet é um software que executa um ataque de negação de serviço.

B) Adware é um software que exibe conteúdo publicitário em seu computador, muitas vezes sem o consentimento do usuário.

C) DoS é um tipo de malware que monitora e captura o que é digitado em um computador.

D) Pharming é uma tentativa de envio de SPAM em massa que utiliza uma rede de computadores.

E) Phishing é uma forma de mascarar o endereço de um site, fazendo com que o endereço de um site falso se passe pelo endereço de um site legítimo.

64. (IADES/TER-PA - 2014) Programas maliciosos de computador podem colocar em risco a integridade dos sistemas que nele rodam e também podem proporcionar acesso indevido a informações sigilosas que ele contenha. Em sistemas Linux, é correto afirmar que os hackers costumam utilizar um software de invasão chamado

A) rootkit.

B) spyware.

C) vírus.

D) malware.

E) keylogger.

65. (FGV/CGE-MA - 2014) A segurança na Internet constitui atualmente uma das preocupações dos administradores de redes, pelos danos que as pragas virtuais podem causar. Nesse contexto, analise as descrições a seguir.

I. São malwares que necessitam de uma interação do usuário para infectar uma máquina. O exemplo clássico é um anexo de e-mail contendo um código executável malicioso. Se o usuário receber e abrir tal anexo, o malware será executado na máquina.

II. São malwares capazes de entrar em uma máquina sem qualquer interação do usuário. O exemplo clássico é o de um usuário que está executando uma aplicação de rede frágil para o qual um atacante pode enviar um malware, que varre a Internet em busca de outros hospedeiros que estejam executando a mesma aplicação de rede vulnerável.

Essas descrições definem, respectivamente, os seguintes termos:

A) worm e sniffer.

B) vírus e worm.

C) proxy e vírus.

D) spyware e proxy.

E) sniffer e spyware.

66. (IMA/Prefeitura de Canavieira-PI - 2015) É um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador:

A) Worm.

B) Firewall.

C) Sniffer.

D) Spyware.

67. (FGV/DPE-MT - 2015) "Teclado Virtual" é uma técnica muito utilizada em aplicações via Internet que demandam maior segurança, como, por exemplo, entrada de senhas de banco ou cartões de crédito em transações bancárias. A ideia é que caracteres não sejam digitados pelo teclado físico e sim clicados com o auxílio do mouse em um teclado virtual que aparece na tela do computador. Seu principal objetivo é combater artefatos maliciosos conhecidos como

A) sniffers.

B) backdoors.

C) worms.

D) keyloggers.

E) rootkits.

68. (IBFC/EBSERH - 2015) "Quando algum sistema operacional efetua um pedido de leitura de um arquivo, ele intercepta os dados que são requisitados e faz uma filtragem dessa informação, deixando o sistema ler apenas arquivos não infectados. Desta forma, o antivírus ou qualquer outra ferramenta ficam impossibilitados de encontrar o arquivo malicioso". Essa definição refere-se ao malware denominado:

A) exploit

B) rootkit

C) sniffer

D) quantum

E) adware

69. (CESPE/TCE-PA - 2016) Os bots, programas de computador que executam operações na forma de agentes em nome de um atacante, podem ser controlados remotamente e são capazes de, entre outras atividades, enviar spam.

70. (VUNESP/MPE-SP - 2016) Existem diversos tipos de malwares que podem infectar e prejudicar os computadores. O tipo de malware que se disfarça como programas legítimos para ser instalado nos computadores pelos usuários é denominado

A) Backdoor.

B) Hijacker.

C) Spyware.

D) Trojans.

E) Worms.

71. (FEPESE/Prefeitura de Lages-SC - 2016) Com relação à instalação e configuração de softwares de segurança, sobre ransomware, assinale a alternativa correta.

A) É um tipo de vírus que geralmente exclui ou troca de lugar (pasta) arquivos de usuário, como planilhas e documentos, do computador infectado.

B) É um tipo de malware ou vírus que geralmente criptografa os arquivos do computador infectado, impossibilitando sua abertura ou visualização.

C) É um tipo de malware ou vírus que realiza o monitoramento das atividades do computador infectado, com o objetivo de capturar senhas ou informações de cartões de crédito, por exemplo.

D) É um tipo de malware que instala um aplicativo no computador infectado com o objetivo de lançar ataques de negação de serviço a partir deste computador, dificultando a localização e rastreamento do agressor, e aumentando seu poder de processamento.

E) É um mecanismo de segurança e constitui uma resposta às tentativas de hackers e invasores de instalar malware no computador, reconhecendo e neutralizando esse tipo de ameaça digital.

72. (FCC/TER-PR - 2017) Um ataque massivo de hackers afetou empresas de diversos países do mundo. Até o momento, companhias de várias áreas de atuação, como comunicação, saúde e finanças foram prejudicadas. De acordo com informações da BBC, Estados Unidos, China, Rússia, Itália e Vietnã têm problemas similares com computadores 'sequestrados' por um tipo de vírus. Há ainda relatos de problemas na Espanha e Portugal.

Além de companhias como Vodafone, KPMG e Telefónica, o serviço de saúde britânico NHS também foi atingido por criminosos virtuais, de acordo com informações da agência Reuters. Ainda segundo a agência, o sistema de saúde do Reino Unido está respondendo aos ataques e, por conta dessa situação, diversos hospitais ao redor do país cancelaram consultas e atendimentos.

Os criminosos infectam as máquinas e demandam um resgate para 'liberar' os dados bloqueados. Alguns relatos informam que os malwares estão cobrando US$ 300 para liberar cada um dos computadores sequestrados e pedem o pagamento em bitcoins. Na rede social Twitter, vários usuários compartilharam imagens de suas telas de computadores após o sequestro. De acordo com relatos, o malware chega por e-mail e afeta, até então, apenas computadores com o sistema operacional Windows. (Adaptado de http://noticias.r7.com/tecnologia-e-ciencia/internet-sob-alerta-ataque-hacker-derruba-sistemas-de-empresas-em-todo-o-mundo-12052017)

Esse tipo de ataque é chamado

A) ransomware.

B) spoofing.

C) sniffing.

D) defacement.

E) DoS.

73. (CONSULPLAN/TJ-MG - 2017) Códigos maliciosos (malwares) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. O programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim é conhecido como:

A) Backdoor.

B) Spyware.

C) Worm.

D) Rootkit.

74. (FCC/TST - 2017) Um usuário notou que o computador ficou demasiadamente lento após a abertura de um e-mail recebido pela internet. Considerando esse sintoma de infecção e que colegas alegaram que receberam e-mails duvidosos desse usuário, trata-se de um malware do tipo

A) Backdoor.

B) Spyware.

C) Worm.

D) Rootkits.

E) Trojan.

75. (CESPE/ABIN - 2018) Uma das características das estruturas de comando e controle de malware descentralizadas é a garantia da existência de uma quantidade significativa de nós redundantes que devem ser atacados para que a rede de comando e controle associada ao malware seja desativada.

76. (FCC/DPE-AM - 2018) O ataque do tipo Distributed Denial of Service - DDoS se utiliza de vários computadores conectados à rede para interromper os serviços da rede e dos equipamentos conectados a ela. Desta forma, para que ocorra um ataque DDoS é necessário que o atacante adquira o controle dos computadores tornando-os escravos, e para isso, utilizar um código malicioso do tipo

A) Spyware.

B) Botnet.

C) Adware.

D) Cavalo de Tróia.

E) Rootkit.

77. (CESPE/STJ - 2018) Fileless malware tem por principal característica a ocultação do endereço de entrada localizado no setor de início do ponto de montagem do sistema de arquivo do disco rígido.

78. (CESPE/STJ - 2018) Ransomware é um tipo de malware que cifra os arquivos armazenados no computador da vítima e solicita um resgate para decifrá-los.

79. (UFRR/UFRR - 2019) É um tipo de malware feito para extorquir dinheiro de sua vítima. Esse tipo de cyber ataque irá criptografar os arquivos do usuário e exigir um pagamento para que seja enviada a solução de descriptografia dos dados da vítima. O scareware é seu tipo mais comum e usa táticas ameaçadoras ou intimidadoras para induzir as vítimas a pagar. O texto acima se refere ao:

A) Spyware

B) Botnet

C) Spam

D) DDoS

E) Ransomware

GABARITO



1. D
2. C
3. D
4. C
5. B
6. E
7. Errado
8. D
9. C
10. A
11. E
12. E
13. A
14. B
15. D
16. A
17. D
18. C
19. Errado
20. E
21. D
22. Errado
23. A
24. Certo
25. D
26. E
27. D
28. B
29. C
30. A
31. D
32. Certo
33. E
34. Errado
35. B
36. D
37. D
38. Errado
39. C
40. D
41. Errado
42. E
43. B
44. B
45. D
46. B
47. C
48. C
49. Errado
50. D
51. Errado
52. Errado
53. B
54. B
55. B
56. B
57. B
58. D
59. A
60. E
61. Errado
62. Errado
63. B
64. A
65. B
66. A
67. D
68. B
69. Certo
70. D
71. B
72. A
73. A
74. C
75. Certo
76. B
77. Errado
78. Certo
79. E

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.