**Segurança**

O**Parkeriano,** ou Parkerian hexad: é um conjunto de seis elementos da segurança da informação proposto por Donn B. Parker. O hexagrama Parkeriano soma mais três atributos aos três atributos clássicos de **segurança** do**triângulo** CIA (confidentiality, integrity, availability ou em português: Confidencialidade, integridade e disponibilidade; estes são os princípios fundamentais da segurança).

Os atributos do hexagrama Parkeriano são os seguintes:

**1. Confidencialidade.**

**2. Posse ou controle.**

**3. Integridade.**

**4. Autenticidade.**

**5. Disponibilidade.**

**6. Utilidade**

O Hexagrama Parkeriano foi proposto por Donn B. Parker e visa expandir os atributos da Tríade de Segurança:

* **Autenticidade** – busca verificar a veracidade quanto à alegação de origem ou autoria de um dado documento ou informação, que poderia ser aferida com o uso de assinatura digital;
* **Posse ou Controle** – quando o dado, informação ou sistema esta na posse de quem o controle ou utiliza. Um cartão de banco roubado pode ser usado sem o consentimento de seu proprietário, que perdeu assim o controle e a posse sobre o cartão;
* **Utilidade** – diz respeito ao proveito que o usuário pode fazer de dados, informações ou sistemas. Um arquivo criptografado cuja chave foi perdida tem sua utilidade comprometida.

**Ataque STP – Spanning Tree Protocol**

STP é um protocolo de gerenciamento de link, que fornece redundância de caminhos, evitando loops indesejáveis na rede. E topologia é a forma q eles estão organizados.

Imagine a seguinte situação: A e B são 2 swtches em uma empresa. Neste caso, não ha como haver loops, pois há apenas um caminho entre A e B.

Agora, imagine que a empresa deseja criar um caminho redundante entre os switches A e B para; caso 1 porta fique inoperante por algum motivo, haja uma segunda rota e a comunicação não seja interrompida. Logo, a situação passa a ser a seguinte:

Um novo problema surge agora, pois, quando A enviar um quadro para B, este vai devolver o quadro para A q, recebendo-o, mandará para B e assim infinitamente,

O STP possibilita que switches se comuniquem a fim de evitar tal situação. Com o STP, os switches trocam informações para criar uma topologia livre de loops por mais que haja mais de um link entre dois switches. O processo inicia com a eleição de um switch raiz(esse processo envolve a troca de bpdus entre todos os switches na rede até um ser eleito - geralmente o que tem o MAC mais baixo).

Finalizada a eleição e a escolha do ladrão, digo, do político, digo, do switch raiz, o STP então deixa apenas o melhor caminho habilitado e bloqueia todos os outros caminhos. Porém caso o caminho que está encaminho o trafego para de funcionar, a topologia e refeita e outro caminho é ativo.

Agora, vamos ver como um ataque ao STP funciona. Ao atacar o protocolo Spanning-Tree, o atacante se passa por um switch e começa enviar BPDUs de melhor prioridade, fazendo o STP recalcula sua topologia e o atacante passará a ser a root bridge da topologia e passará a receber todo o trafego comutado entre os switches, Esse ataque é possível devido ao fato do STP não exigir autenticação dos BPDUs trocados entre os switches.

**Ataques de Amplificação DNS**

**O DNS (Domain Name System) é um sistema de gerenciamento de nomes para identificação de computadores, serviços ou qualquer recurso, usado na Internet e em redes locais. Ele associa nomes para endereços IP e endereços IP para nomes. Há servidores DNS autoritativos e recursivos. Os servidores autoritativos possuem armazenadas associações entre nomes de domínio e endereços IP, e os servidores recursivos recebem as requisições de um cliente e enviam requisições a outros servidores DNS para descobrir o endereço IP do domínio solicitado.**

**Em um ataque de amplificação DNS, é enviado um grande número de solicitações para um ou mais servidores de nomes, usando-se um endereço IP de origem mascarado com o IP da vítima. Com o IP de origem mascarado, o servidor envia as respostas à vítima. Essas respostas são de tamanhos maiores que as requisições. Com a adoção das DNSSEC (DNS Security Extensions), as respostas dos servidores DNS passaram a carregar chaves criptográficas e assinaturas digitais, o que aumenta o tamanho da resposta. Além disso, se a requisição for do tipo “ANY”, que solicita todas as informações sobre um domínio, o tamanho da resposta é ainda maior. Dessa forma, mesmo que os atacantes tenham baixas larguras de banda, eles podem causar grandes impactos na máquina-alvo e na rede que ela está utilizando.**

**Para enviar essas requisições, é usado o protocolo UDP (User Datagram Protocol), que não é orientado à conexão, ou seja, que não possui confirmações de entrega e confirmação do remetente por apresentação (handshake). O uso desse protocolo combinado com o fato de que há vários servidores recursivos que aceitam requisições de qualquer IP, chamados de resolvedores abertos (ou open resolvers), na Internet, torna difícil bloquear esse tipo de ataque.**

**Footprinting:** É o levantamento das informações do alvo, footprint significa pegada, então a etapa de footprinting seria como achar "as pegadas", o "caminho das pegadas" do alvo na internet; É uma fase de coleta de informações sobre o alvo. O footprinting pode ser feito manualmente ou por programas; Uma etapa de planejamento de um ataque.

Footprinting (ou Footprint) é uma **etapa de um ataque** a computadores. Para se executar um ataque a computadores e a redes de computadores, geralmente são cumpridos vários passos, como os listados abaixo:

* 1 - Footprinting
* 2 - Varreduras
* 3 - Enumeração de vulnerabilidades
* 4 - Ataque
* 5 - Cobertura de rastros
* 6 - Manutenção do acesso

No mais, **Black Box** (Caixa Preta) é quando não se tem conhecimento da estrutura do software/rede/dispositivo/empresa a ser alvo do Pentest (Teste de Penetração / Teste de Invasão). E **White Box** (Caixa Branca) é quando se tem algum conhecimento da estrutura interna do software/rede/dispositivo/empresa alvo, o que facilita as coisas.

**Footprint**: Busca detalhada de informações sobre o alvo para uma intrusão Alguns Objetivos do **Footprint:**

* Levantamento de Informações de Domínios: Nomes de domínios, Responsáveis pelos domínios, Servidores de domínios.
* Identificação do Sistema Operacional da máquina-alvo **(Fingerprint).**

**Honeypot** é uma ferramenta ou sistema criado com objetivo de enganar um atacante e fazê-lo pensar que conseguiu invadir o sistema, quando na realidade, ele está em um ambiente simulado, tendo todos os seus passos vigiados.

Em termos de segurança do computador, um honeypot funciona atraindo os hackers para uma armadilha. É um sistema de computador sacrificial que pretende atrair ciberataques, como uma emboscada. Ele emula um alvo para os hackers e usa suas tentativas de intrusão para obter informações sobre cibercriminosos e a maneira como eles estão operando ou para distraí-los de outros alvos.

**Ferramentas antimalware** são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.

Há diversos tipos de programas antimalware que diferem entre si das seguintes formas: pelo método de detecção, pela forma de obtenção, pela execução e pelas funcionalidades apresentadas.

Os métodos de detecção mais comuns são:

* Assinatura (uma lista de assinaturas é usada à procura de padrões);
* **Heurística (baseia-se nas estruturas, instruções e características que o código malicioso possui)** e;
* Comportamento (baseia-se no comportamento apresentado pelo código malicioso quando executado).

Fonte: Cartilha de Segurança para Internet - CERT.br.

**Stealth (ou furtivo) é o termo que se usa para descrever técnicas usadas para tornar o malware invisível. Ou seja, disfarçar quaisquer modificações que o malware possa fazer no sistema infectado. Isso inclui, por exemplo, rootkits.** Vírus Steatlth são malwares que utilizam técnicas de programação para evitar a detecção por ferramentas de segurança. Os vírus tentam matar as tarefas associadas ao software antivírus antes que seja detectado.

**IDS ➜ Sistema de Detecção de Intruso**

* Age passivamente.
* Monitorar o tráfego da rede
* Não bloqueia uma ação, mas **verifica** se esta ação é ou não uma ameaça
* Não interfere no fluxo de tráfego da rede.

**IPS ➜ Sistema de Prevenção de Intruso**

* Age ativamente.
* Complemento do IDS
* Identifica uma intrusão, analisa a relevância do evento/risco
* **Bloqueia** determinados eventos
* O IPS usa a capacidade de detecção do IDS junto com a capacidade de bloqueio de um firewall
* Age em diversos pontos de uma arquitetura de rede.

**Sistemas de Detecção de Intrusão baseados em Rede** (NIDS) monitora e analisa todo o tráfego no segmento da rede. Consiste em um conjunto de sensores que trabalha detectando atividades maliciosas na rede, como ataques baseados em serviço, portscans, etc… São instalados em máquinas responsáveis por identificar ataques direcionados a toda a rede, monitorando o conteúdo dos pacotes ou do tráfego e seus detalhes como informações de cabeçalhos e protocolos. Os **NIDS** têm como um dos objetivos principais detectar se alguém está tentando entrar no seu sistema ou se algum usuário legítimo está fazendo mau uso do mesmo.

**Time Bomb (Bomba Logica)** conhecido como **“Bomba Relógio”,** é uma ameaça programada para ser executada em um determinado momento no sistema operacional, causando-lhe danos, se instalam silenciosamente e agem apenas em datas ou momentos determinados, que são definidos pelo seu criador.

**Vírus:**é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus **depende da execução** do programa ou arquivo hospedeiro.

* **Vírus Polimórficos:** são capazes de criar uma nova variante a cada execução, mudam a sua assinatura para dificultar a detecção pelo antivírus.
* **Vírus Metamórficos:** são capazes de mudar o próprio corpo, evitam gerar instâncias parecidas com a anterior. Reescrevem-se completamente, mudando a assinatura, o tamanho e até o próprio comportamento.

**Worm:**é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

**Botnet:**é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

**Backdoor: é** um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

**Pharming:** 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. Quando você tenta acessar um site legítimo, o seu navegador web é redirecionado, de forma transparente, para uma página falsa. Com isso, suas credenciais de acesso podem ser capturadas para uso malicioso.

De acordo com Wikipedia, **pharming é o termo atribuído ao ataque baseado na técnica DNS cache poisoning (envenenamento de cache DNS)** que, consiste em corromper o DNS (Sistema de Nomes de Domínio ou Domain Name System) em uma rede de computadores, fazendo com que a URL (Uniform Resource Locator ou Localizador Uniforme de Recursos) de um site passe a apontar para um servidor diferente do original. Os golpistas geralmente copiam fielmente as páginas das instituições, criando a falsa impressão que o usuário está no site desejado e induzindo-o a fornecer seus dados privados como login ou números de contas e senha que serão armazenados pelo servidor falso.

Ou seja, no ataque pharming utiliza-se a técnica de DNS cache poisoning, que é o envenamento de cache DNS. E lembrando que pharming é um tipo especifico de phishing.

**Tipos de Trojan**

* **Trojan Downloader:** instala outros códigos maliciosos, obtidos de sites na Internet.
* **Trojan Dropper:** instala outros códigos maliciosos, embutidos no próprio código do trojan.
* **Trojan Backdoor:** inclui backdoors, possibilitando o acesso remoto do atacante ao computador.
* **Trojan DoS:** instala ferramentas de negação de serviço e as utiliza para desferir ataques.
* **Trojan Destrutivo:** altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
* **Trojan Clicker:** redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.
* **Trojan Proxy:** instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.
* **Trojan Spy:** instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.
* **Trojan Banker ou Bancos:** coleta dados bancários do usuário, através da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados. É similar ao Trojan Spy porém com objetivos mais específicos.

**Smurf** é uma forma de [ataque de negação de serviço distribuído (DDoS)](https://www.kaspersky.com.br/resource-center/threats/ddos-attacks) que deixa as redes de computadores inoperáveis. Para fazer isso, o programa Smurf [explora vulnerabilidades](https://www.kaspersky.com.br/resource-center/threats/malware-system-vulnerability) dos protocolos IP e ICMP.

Um ataque Smurf segue estas etapas:

* Primeiro, o [malware](https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it) cria um pacote de rede anexado a um endereço IP falso, uma técnica conhecida como "spoofing", ou falsificação.
* Dentro do pacote, há uma mensagem de ping por ICMP solicitando que os nós de rede que receberem o pacote enviem uma resposta de volta
* Essas respostas, ou "ecos", são retornadas a endereços IP da rede, entrando em um loop infinito.

Quando combinado com uma transmissão de IP, que envia o pacote malicioso para todos os endereços IP na rede, o ataque Smurf é capaz de causar rapidamente uma negação de serviço completa.

**Como se proteger**

O ataque Smurf parece inofensivo, mas apresenta riscos reais quando sobrecarrega os servidores. Com uma transmissão de IP desabilitada e ferramentas de detecção confiáveis, você limita a chance e o impacto desse ataque. Seguem alguns procedimentos para atenuar o ataque do Smurf:

* bloqueie o tráfego de transmissão direcionada que chega à rede
* configure hosts e roteadores para que não respondam a solicitações de eco do ICMP.

**Browser Hijacker** é um software malicioso que modifica o registro do sistema operacional, alterando o funcionamento do navegador, modificando sua página inicial, abrindo páginas automaticamente ou inserindo botões inadvertidamente.

(Q1054830) Os programas que alteram a página inicial do navegador e também são capazes de redirecionar qualquer página visitada para outra, escolhida pelo criador da praga, são denominados de: Hijackers. **CERTO.**

**SYN Flood (ou de fragmentação)** é um método de ataque DDoS que causa uma sobrecarga direta na camada de transporte (camada 4) e indireta na camada 7 (camada de aplicação).Como funciona? Para entender como esse ataque funciona, é preciso primeiramente entender alguns conceitos:

##### **Protocolo TCP** - Para que uma conexão confiável seja estabelecida entre o usuário e o servidor, eles precisam se apresentar através do protocolo TCP (*Transmission Control Protocol*). O mecanismo de estabelecimento e finalização de conexão ocorre em três etapas e é chamado de *Three-Way Handshake*.

* **Three-Way Handshake** - Primeiro, o usuário requisita uma conexão enviando um pacote SYN (*synchronize*) ao servidor. Em seguida, o servidor envia um SYN-ACK (*acknowledge*) de volta ao cliente reconhecendo e confirmando o recebimento da requisição. Por fim, o cliente então responde com um ACK, estabelecendo a conexão.
* ***Ataque SYN Flood -***Neste tipo de ataque, o atacante envia milhares de pacotes SYN ao servidor alvo com endereços IP ilegítimos. O servidor então envia um SYN-ACK de confirmação ao falso usuário e fica aguardando a sua resposta para validar a conexão. Entretanto, essa resposta nunca chega e o *Three-Way Handshake* não é completado. Um grande volume de pacotes SYN pode estourar o limite de conexões TCP que o servidor/serviço consegue manter ativas simultaneamente, sobrecarregando a capacidade computacional e causando uma indisponibilização do servidor/serviço e deixando usuários legítimos impossibilitados de se conectar.

**Ataque de dia zero** refere-se a um servidor ou programa com uma vulnerabilidade prévia **desconhecida**, não corrigida antecipadamente. Atacantes podem aproveitar-se da vulnerabilidade e atacar o servidor ou programa. Um exploit é um pedaço de software, um pedaço de dados ou uma sequência de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento acidental ou imprevisto a ocorrer no software ou hardware de um computador ou em algum eletrônico. Então um atacante explora as vulnerabilidades de um sistema, no dia zero. Questão: Como é conhecido o ataque que explora uma vulnerabilidade previamente desconhecida? Resposta: Ataque de dia zero.

Uma vulnerabilidade de **dia zero** é uma falha de software, hardware ou firmware desconhecida pelo fabricante. Quando os hackers se aproveitam dessa falha para realizar um ataque cibernético, isso é chamado de exploração do **dia zero.**

Os ataques de dia zero são capazes de devastar uma rede, explorando as vulnerabilidades das aplicações envolvidas.

Uma vez que a falha Dia Zero é descoberta e divulgada, o desenvolvedor do programa lançará uma correção o mais rápido possível. Portanto, a melhor forma de proteger sua empresa é manter todos os softwares instalados e o sistema operacional sempre atualizado.

**Ransomware:**O malware que, por meio de criptografia, torna inacessíveis os dados armazenados em um equipamento e exige pagamento de resgate para restabelecer o acesso ao usuário. Ransomware é um tipo de malware que cifra os arquivos armazenados no computador da vítima e solicita um resgate para decifrá-los. **A forma mais comum de infectar um computador com ransomware é utilizando a técnica de phishing** para enganar a vítima, fazendo com que ela clique em um link enviado via e-mail que ache ser confiável.

***Jamming*é o alagamento de freqüências de rádio com um sinal indesejado. O resultado ea indisponibilidade do sinal necessário para dispositivos sem fio. Desde há muito ruído no ar, o usuário válido não pode tomar o sinal correto. Questão: Um tipo de ataque em redes sem fio é conhecido como Jamming, que tem como forma de atuação: nundar a região geográfica atacada com sinal de radiofrequência na frequência dos canais da rede sem fio.**

**O ataque KRACK** (*key reinstallation attack*) - explora uma fragilidade no handshake do protocolo WPA2 (Wi-Fi Protected Access II), que é usado para estabelecer uma chave de criptografia para criptografar o tráfego...

...O ataque funciona contra o protocolo WPA1 e o WPA2 e contra qualquer conjunto de cifras que esteja sendo usado (WPA-TKIP, AES-CCMP e GCMP).O KRACK permite que os atacantes tenham acesso a chave de criptografia utilizada na rede e assim desencriptem os pacotes navegando na rede Wi-Fi. A senha da rede Wi-Fi não é exposta, mesmo assim o ataque permite capturar todos os pacotes de rede, e assim ter acesso a todas as comunicações dos usuários (exceto acessos criptografados, como SSL, VPN, SSH, etc), além de injetar pacotes na rede wireless da vítima...

...Segundo os pesquisadores, esse ataque é excepcionalmente devastador contra equipamentos rodando Linux e Android versão 6.0 ou superior, pois eles podem ser enganados para reinstalar uma chave de criptografia com valor totalmente zero...

**CSRF:**Consiste em inserir requisições em **uma sessão já aberta pelo usuário, explorando a confiança que um site tem do navegador**. Atua após a obtenção do cookie gerado pela aplicação após a autenticação. Por meio do cookie, o servidor acredita estar se comunicando com o usuário real e autenticado. Pode ser inibido por captcha.

**CSS/XSS:** Ataque baseado em induzir o navegador web do usuário a executar um script malicioso dentro do contexto de um site confiável. A exploração bem sucedida deste permite ao hacker embutir um código malicioso (na forma de JavaScript, geralmente) em campos de entrada, os quais serão inseridos de volta para a resposta do servidor

**Diferença entre XSS e CSRF:**

* XSS tira proveito da confiança que o usuário tem no site. Explora o usuário/navegador.
* CSRF tira proveito da confiança que o site tem no usuário. Explora o site/sessão

**Sequestro de Sessão (Session Hijacking)** - O seqüestro de sessão é sinônimo de uma sessão roubada, na qual um invasor intercepta e assume uma sessão legitimamente estabelecida entre um usuário e um host. Uma vez que aconteça um sequestro de sessão bem-sucedido, o invasor pode assumir o papel do usuário legítimo ou simplesmente monitorar o tráfego para injetar ou coletar pacotes específicos a fim de criar o efeito desejado.

Segundo o Navathe [1], na página 576, há 3 tipos de Sql Injection: Manipulação de SQL, Injeção de código, Injeção de chamada de função. O livro define os tipos da seguinte forma:

**Manipulação de SQL:** Um ataque de manipulação, que é do tipo mais comum de ataque de injeção, muda um comando SQL na aplicação - por exemplo, ao acrescentar condições a cláusula WHERE de uma consulta, ou ao expandir uma consulta com componentes de consulta adicionais, usando operações de união como UNION, INTERSECT ou MINUS.  
**Injeção de código:** Esse tipo de ataque tenta acrescentar instruções SQL ou comandos adicionais à instrução SQL existente, explorando um bug de computador, que é causado pelo processamento de dados inválidos. O atacante pode injetar ou introduzir código em um programa de computador para alterar o curso da execução. A injeção de código é uma técnica popular para a invasão ou penetração do sistema para obter informações.  
**Injeção de chamada de função:** Nesse tipo de ataque, uma função do banco de dados ou uma chamada de função do sistema operacional é inserida em uma instrução SQL vulnerável para manipular os dados ou fazer uma chamada privilegiada. Por exemplo, é possível explorar uma função que realiza algum aspecto relacionado à comunicação na rede."

***Blind* SQL *injection*** tem por característica a exploração de perguntas ao banco de dados, as quais retornam verdadeiro ou falso; conforme a resposta da aplicação, o atacante consegue identificar de onde os dados podem ser extraídos do banco, por falhas de programação na aplicação. O**Blind SQL Injection,** ou Injeção de SQL as Cegas é o que separa meninos de homens na área de segurança da informação e Pentests de ambientes Web, pois o melhor ferramental que você pode ter em mãos é o seu próprio conhecimento de SQL e servidores web para extrair dados a força do servidor. Em uma linguagem mais precisa, os ataques de SQL Injection normais, quando enviamos os parâmetros de consulta para a base de dados para extrair informação, nos retornam erros e informações pertinentes na tela, o **Blind SQL Injection não nos retorna nada. A partir disso só nos resta interpretar valores de lógica booleana (True e False)**