**PenTest** - Inicialmente temos que entender que pentest é um serviço, de preferência legalizado e extremamente necessário para qualquer empresa que necessite proteger dados sensíveis.

As organizações possuem necessidades grandes em manter informações online e a preocupação que estas informações estejam, de certa forma, protegidas de quaisquer pessoas que não estão autorizadas a acessá-las.

Junto com essa necessidade, começaram a surgir serviços que simulam ataques hackers para testar estas vulnerabilidades e então corrigi-las.

Este tipo de serviço está diretamente ligado à área se segurança da informação, onde empresas contratam diferentes profissionais (hackers) para a realização de diversos teste à procura de falhas em seus sistemas, redes e/ou serviços, e posteriormente documentam as falhas encontradas para análise e correção.

**Necessidades PenTest**

* Testar as vulnerabilidades da empresa.
* Testar o time de resposta à incidentes de Segurança.
* Testar o monitoramento.
* Testar regras de firewall.
* Testar o nível de maturidade dos usuários.
* Testar determinadas aplicações.

**Tipos de PenTest**

* **Black Box(Blind)** - Neste tipo de ataque o auditor não conhece nada sobre o alvo que irá atacar, porem o alvo sabe que será atacado e o que será feito durante o ataque.
* **Double Black Box(Double Blind)** - Neste tipo de ataque o auditor não conhece nada sobre o alvo, e o alvo não sabe que será atacado e tão pouco quais testes serão realizados.
* **Gray Box** - Neste tipo de ataque o auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado e também sabe quais testes serão realizados. Este é o tipo de pentest mais realista possível, ataque real.
* **Double Gray Box** - Neste tipo de ataque o auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado, porém, não sabe quais testes serão executados.
* **Tandem** - Neste tipo de ataque o auditor tem total sobre o alvo, e o alvo sabe que será atacado e também o que será testado. Este tipo de ataque também é conhecido como “Caixa de cristal”.
* **Reversal** - Neste tipo de ataque o auditor tem conhecimento total do alvo, porém o alvo não sabe que será atacado, e tão pouco quais teste serão executados. Este tipo de ataque é ideal para testes a capacidade de resposta e como esta o timing de ação da equipe de resposta a incidentes do alvo.

**Visão Macro**

1. Encontrar um cliente
2. Efetuar uma reunião comercial apresentar a sua empresa.
3. Enviar as propostas Técnicas e Comercial.
4. Em caso de aprovação, efetuar o Trabalho.
5. Apresentar o relatório com as vulnerabilidades.

**Na sua Visão**

1. Encontrar um possível cliente.
2. Estudar o ramo de atividade do cliente.
3. Conseguir uma reunião comercial.
4. Ouvir as necessidades do clientes.
5. Elaborar a proposta de acordo com o ambiente do cliente.
6. Solicitar ao cliente um mapa de sua rede, sistemas operacionais e conexões.
7. Montar o projeto de acordo com o ambiente e necessidade do cliente.
8. Enviar as propostas técnicas e comerciais.
9. Cobrar o cliente caso o mesmo não retorne em 72h.
10. Em caso de aprovação, preparar as ferramentas adequadas para o projeto.
11. Preparar junto com o cliente a linha do tempo e segui-lá à risca.
12. Apresentar relatório final.

**Ética Hacker** é o termo que descreve os valores morais e filosóficos na comunidade hacker. É importante seguir seus princípios, porém, devemos lembrar que não podemos em hipótese alguma infringir as regras de seus clientes.

**Os temas das Ética Hacker são:**

* Compartilhamento
* Abertura
* Descentralização
* Livre acesso aos computadores
* Melhoria do mundo

Para iniciarmos o serviço de **PenTest**, devemos efetuar 3 processos obrigatórios:

1. **Efetuar o processo de Varredura**
2. Realizar Scans de sistemas operacionais
3. Identificar serviços e suas versões
4. Identificar Redes e IPs
5. Procurar por arquivos desprotegidos
6. **Identificar e enumerar as vulnerabilidades**
7. Procurar por exploits
8. Verificar portas abertas de forma insegura
9. Procurar por serviços publicados de forma insegura
10. Procurar por senhas fracas
11. Procurar por erros de configuração e programação

3. **Efetuar a exploração e documenta-las**

1. Explorar falhas encontradas
2. Escalar privilégios
3. Documentar acessos indevidos
4. Efetuar Bypass de sistemas de proteção
5. Enumerar e documentar falhas encontradas

**Relatório linha do tempo:** É onde você descreve o que fará e o que já fez. Siga rigorosamente esta linha do tempo para evitar processos ou problemas a você ou seu cliente. Não existe um modelo especifico, pois, cada projeto deve seguir um modelo diferenciado. O importante é que no seu relatório de linha do tempo, tenha o que chamamos de transbordo, ou seja, são algumas horas adicionais que serão usadas caso você tenha problemas ao decorrer das previsões anteriores, esse transbordo não poderá ultrapassar 20% das horas do projeto.

Exemplo:

**Scan - Dia 01/06**

File Server

08h - 12h

Print Server

13h - 14h

Active Directory

14h - 17h

Oracle - DBA - INFRA

17h - 20h

**Entendendo o Cliente** - O objetivo da primeira reunião comercial é entender as necessidades do cliente, com isso, você deve anotar todas as necessidades de seu cliente. Não pode se apresentar uma proposta na primeira reunião, caso contrário, você poderá cobrar um valor irregular e poderá prejudica-lo e prejudicar seu cliente.

**Os limites de seu cliente**

Seu cliente, dependendo do ramo de atividade, possui limites, ou seja, existem servidores, horários e ambientes ao qual você não poderá auditar.

Após a aprovação do seu projeto, reúna-se com seu cliente e levante as seguintes informações:

1. Quais dispositivos não podem ser auditados
2. Quais redes não podem ser auditadas
3. Quais dados são sensíveis a Pentesters
4. Quais os horários de cada varredura

Crie uma lista de servidores e estações que não podem ser auditados, é comum que ao efetuar alguma varredura, alguns serviços param de funcionar, seu cliente deve estar ciente disso em contrato !

**Elaborando proposta técnica** - Deve ser enviada ao Gerente técnico, administrador de redes ou Security Officer

Deverá contar os seguintes itens:

1. O que será auditado
2. As ferramentas utilizadas
3. Os testes realizados (SQLi, Brute Force, Bypass antivírus, etc)
4. Em caso do uso de OWASP, especificar quais ataques
5. Não enviar o valor do projeto nesta proposta

**Elaborando proposta comercial** - Será enviada ao Diretor da área ou ao contratante. Nele irá obter o valor do projeto, seja ele por hora projeto ou comissão.

Não deve conter conteúdo técnico neste proposta, no máximo você poderá dizer que tipo de pentes irá realizar.

**Protocolo TCP**

O TCP (que significa Transmission Control Protocol, em português: Protocolo de Controle de Transmissão) é um dos principais protocolos da camada de transporte do modelo TCP/IP. Ele permite, a nível das aplicações, gerir os dados em proveniência da(ou com destino à) camada inferior do modelo(ou seja, o protocolo datagramas IP,fixando o campo protocolo em 6(para saber que o protocolo ascendente é o TCP...). O TCP é um protocolo orientado para a conexão, isto é, ele permite a dias máquinas comunicantes, controlar o estado da transmissão.

As principais características do protocolo TCP são:

* TCP entrega ordenadamente os datagramas provenientes do protocolo IP.
* TCP verifica a onda de dados para evitar uma saturação da rede.
* TCP formata os dados em segmentos de comprimento variável para “entrega-los” ao protocolo IP.
* TCP permite o multiplex dos dados, quer dizer, faz circular, simultaneamente, as informações que proveem de fontes (aplicações, por exemplo) distintas numa mesma linha.

**Criando comunicação TCP**

->SYN

<-SYN, ACK(SYN) Servidor -> Cliente

->ACK(SYN) Cliente -> Servidor

**Encerrando comunicação TCP**

-> FIN

<- ACK

<- FIN

-> ACK

**Protocolo UDP**

O **User Datagram Protocol** (UDP) é um protocolo simples da camada de transporte. Ele é descrito na RFC 768 e permite que a aplicação escreva um datagrama encapsulado num pacote IPv4 ou IPv6, e então enviando ao destino. Mas não há qualquer tipo de garantia que o pacote irá chegar ou não.

O protocolo UDP não é confiável. Caso garantias sejam necessárias, é preciso implementar uma série de estruturas de controle, tais como timeouts, retransmissões, acknowlegments, controle de fluxo, etc. Cada datagrama UDP tem um tamanho e pode ser considerado como um registro indivisel, diferentemente do TCP, que é um protocolo orientado a fluxos de bytes sem início e sem fim.

Também dizemos que o UDP é um serviço sem conexão, pois não há necessidade de manter um relacionamento longo entre cliente e o servidor. Assim, um cliente UDP pode criar um socket para um servidor e imediatamente enviar outro datagrama com o mesmo socket para um servidor diferente. Da mesma forma, um servidor poderia ler datagramas vindos de diversos usando um único socket.

**Portas e Serviços**

As portas são extremamente importantes para que haja mais do que 1 comunicação por vez em cada computador. Sendo assim, diversos serviços podem se comunicar simultaneamente através do protocolo TCP ou UDP.

O computador possui 65535 portas TCP e mais 65535 portas UDP.

As principais portas x serviços utilizados são:

21 TCP: FTP

22 TCP: SSH

23 TCP: Telnet

25 TCP: SMTP

53 UDP: DNS

69 UDP: TFTP

80 TCP: HTTP

110 TCP: POP3

123 UDP: NTP

443 TCP: HTTPS

Toda comunicação se faz utilizando portas de Origem e Destino. Geralmente o sistema operacional utiliza as portas de Origem acima de 1024, ou seja são chamadas de portas baixas, todas as portas abaixo de 1024.

**Protocolo ICMP**

ICMP, sigla para o inglês Internet Control Message Protocol, é um protocolo integrante do protocolo IP, definido pelo RFC 792, e utilizado para fornecer relatórios de erros à fonte original. Qualquer computador que utilize IP precisa aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado. Os gateways devem estar programados para enviar mensagens ICMP quando receberem datagramas que provoquem algum erro.

As mensagens ICMP geralmente são enviadas automaticamente em uma das seguintes situações:

* Um pacote IP não consegue chegar ao seu destino (i.e. Tempo de vida do pacote expirado)
* O Gateway não consegue retransmitir os pacotes na frequência adequada (i.e. Gateway congestionado)
* O Roteador ou Encaminhador indica uma rota melhor para a máquina a enviar pacotes.
* Ferramentas comumente usadas baseadas nesse protocolo são: Ping e Traceroute.

Alguns firewalls, geralmente instalados em servidores Windows ou Unix, bloqueiam as respostas (ICMP Reply), dificultando o Ping e o Traceroute (tracert).

Isto por diversas razões. Uma delas é para bloquear os ataques de hackers, que consiste na sobrecarga da memória, enviando dados (em ping) até o sistema não ter capacidade de administrar suas próprias funções.

Esse ataque é significativo, principalmente contra usuários do Microsoft Windows.

**Camada OSI**

O modelo OSI é um modelo de referência da ISO que tinha com principal objetivo ser um modelo padrão, para protocolos de comunicação entre os mais diversos sistemas, e assim garantir a comunicação end-to-end.

Esta arquitetura é um modelo que divide as redes de computadores em 7 camadas, de forma a se obter camadas de abstração. Cada protocolo implementa uma funcionalidade assinalada a uma determinada camada.

O modelo OSI permite comunicação entre máquinas heterogêneas e define diretivas genéricas para a construção de redes de computadores(seja de curta, média ou longa distancia) independente da tecnologia utilizada.

**Camadas:** Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace de Dados, Físico.

**Físico** - Modem, RDS, RS-232, EA-122, RS-449, Bluetooth, USB, 10BASE-T, 100BASE-TX, ISON, SONET, DSL.

**Enlace de Dados**

* Sub camada - LLC
* Sub camada - MAC

Ethernet, 802 11, Wi-Fi, IEEE, 802 1Q 802 11g HOLC Token ring FODI PPP Switch

Frame rolay ATM.

**Rede** - IP(Pv4, IPv6), IPsec, ICMP, ARP, RARP, NAT.

**Transporte** - NotBeui, TCP, UCP, RTP, SCTP, DCCP, RIP.

**Sessão** - NetBios.

**Apresentação** - XDR, TLS.

**Aplicação** - HTTP, SMTP, FTP, SSH, Telnat, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BvTorrent, DNS, Ping.

**Redes NAT**

Em redes de computadores, NAT, Network Address Translation, também conhecido como masquerading é uma técnica que consiste em reescrever, utilizando-se de uma tabela hash, os endereços IP de origem de um pacote que passam por um router ou firewall de maneira que um computador de uma rede interna tenha acesso ao exterior ou Rede Mundial de Computadores (internet).

**Redes Bridge**

O bridge pode ser um dispositivo dedicado ou então um PC com duas placas de rede, configurando para executar esta função.

A primeira vista pode parecer que o bridge tem a mesma função de um hub comum, mas as aplicações são bem diferentes. Um hub permite conectar vários PCs, que passam a fazer parte de um único segmento de rede, onde todos os dados transmitidos por um PC são transmitidos a todos o que diminui o desempenho da rede conforme aumenta o tráfego de dados e a quantidade de PCs.

O bridge é capaz de examinar pacotes e transmitir os pacotes apenas ao destinatário (Ethernet por exemplo) e que utilizem o mesmo protocolo de rede (TCP/IP, por exemplo). Os switches seguidos pelos roteadores são os próximos degraus da escala evolutiva.

**Redes Internas**

Como o próprio nome diz, as redes internas podem ser utilizadas para testes de redes que não influenciam as redes de produção. Tecnicamente é uma rede separada, ao , qual, não faz parte da rede principal no nosso caso.

Quando criamos máquinas virtuais, podemos separa-las para que tenha acesso apenas à uma rede interna, isso fará com que ela seja completamente desconectada da rede principal e principalmente da internet.

Para poder realizar o processo de junção das redes, será necessário a realização de roteamentos ou pontes.

**Entendendo a Virtualização**

Virtualização, basicamente, é a técnica de separar aplicação e sistema operacional dos componentes físicos. Por exemplo, uma máquina virtual possui aplicação e sistema operacional como um servidor físico, mas estes não estão vinculados ao software e pode ser disponibilizado onde for mais conveniente.

Uma aplicação deve ser executada em um sistema operacional em um determinado software.

Com virtualização de aplicação ou apresentação, estas aplicações podem rodar em um servidor ou ambiente centralizado e ser deportada para outros sistemas operacionais e hardwares.

**Kali Linux**

A distribuição Kali Linux é o sistema ideal para todos que trabalham com ferramentas de segurança da informação. Foi desenvolvida pelos mesmos criadores do BackTrack Linux, o mais conceituado sistema para analise de vulnerabilidade e que provavelmente será descontinuado, dando lugar ao novo Kali Linux utilizando o kernel do Derbian como base.

O Kali é uma distribuição completa, baseada em Debian, e que pode ser instalada em qualquer máquina, facilitando assim a atualização das ferramentas que o compõem e que dão suporte às funções de testes de rede e de sistemas. São mais de 300 ferramentas disponíveis e que podem ser utilizadas para avaliar os níveis de segurança de sistemas computacionais e redes.

Kali Linux é uma distribuição Linux GPL compatível construída por testadores de penetração para testadores de penetração.

**Varreduras**

Há 3 tipos de varreduras que podemos utilizar em nosso ambiente para detectar possíveis ataques.

1. **Varreduras Passivas**

As varreduras Passivas, buscam outros métodos de coletar dados do alvo, sendo assim, tornando-se indetectáveis, porém, não tão específicas como as varreduras ativas.

1. **Varreduras** **Ativas**

Quando realizamos varreduras ativas, vamos direto ao alvo, com o objetivo de coletar dados precisos sobre o ambiente atual. Essa técnica é de fácil detecção por Firewalls/IDS/WAFs e afins.

1. **Varreduras Furtivas**

Varreduras Furtivas tem o objetivo de utilizar as técnicas das varreduras ativas, porém, com a menor probabilidade de detecção. Efetuando evasões de sistema de detecção e confundindo os administradores de uma rede.

**Google Hacking**

O Google Hacking envolve o uso de operadores avançados no Google, motor de busca para localizar sequências específicas de texto dentro de resultados de pesquisa. Alguns dos exemplos mais populares são, encontrar versões de pesquisa. Alguns dos exemplos mais populares são, encontrar versões específicas de grupos vulneráveis em aplicações web.

Alguns dos exemplos mais populares é encontrar versões específicas de grupos vulneráveis em aplicações web. As consultas de pesquisas a seguir seriam localizar todas as páginas que possuem um determinado texto contidas na página.

Através do Google Hacking, você pode encontrar particularidades que talvez já tenham até saído do ar. Obtendo um número razoável de informações sobre um determinado alvo, é possível explorar suas vulnerabilidades.

Esta ferramenta é tão robusta que pouco conhecemos sobre ela, primeiramente, devemos entender como o google funciona:

**Varredura Passiva**

**intitle:”Pesquisa”** - Busca apenas páginas que contenham o pesquisado como titulo.

**inurl:”Pesquisa”** - Busca apenas páginas que contenham o pesquisado na URL.

**site:”Pesquisa”** - Busca apenas páginas que contenham o domínio pesquisado.

**filetype:”Pesquisa”** - Busca apenas arquivos que contenham o que foi pesquisado.

**intext”Pesquisa”** - Busca apenas páginas que contenham a palavra pesquisa nos resultados de pesquisa.

**Pesquisa-Palavra que não quero pesquisar** - Busca apenas páginas que não contenham a palavra após o “-”.

**Pesquisa +incremento de pesquisa**

**“Pesquisa Pesquisa”** - Busca apenas páginas que contenham resultado somente na ordem inserida.

**Pesquisa OR Pesquisa** - Busca páginas que contenham somente um dos parâmetros pesquisados.

**Pesquisa AND Pesquisa** - Busca páginas que contenham todas as palavras pesquisadas.

**Seguem lista de dorks mais comuns e suas respectivas falhas:**

**Lista de Dorks para ataques XSS:**

# <http://www.esecurity.com.br/blackhat2/dorks/dorks-xss.txt>

**Lista de Dorks para ataques LFI:**

# [http://www.esecurity.com.br/blackhat2/dorks/dorks-lfi.txt](http://www.esecurity.com.br/blackhat2/dorks/dorks-xss.txt)

**Lista de Dorks para ataques RFI:**

# [http://www.esecurity.com.br/blackhat2/dorks/dorks-rfi.txt](http://www.esecurity.com.br/blackhat2/dorks/dorks-xss.txt)

**Lista de Dorks para ataques SQL:**

# [http://www.esecurity.com.br/blackhat2/dorks/dorks-sql.txt](http://www.esecurity.com.br/blackhat2/dorks/dorks-xss.txt)

**Maltego**

O maltego foi desenvolvido pela empresa PATERVA e roda em sistemas operacionais como Windows, Mac e Linux.

**É capaz de determinar os relacionamentos entre links do mundo real, tais como:**

* Pessoas
* Grupo de Pessoas (Redes Sociais)
* Companhias
* Organizações
* Web Sites

**Infraestrutura interna como:**

* Domínios
* Nomes de DNS
* Netblocks
* Endereços de IP

Há 2 versões do Maltego e uma ferramenta adicional (**CaseFile**)

A versão Community que é gratuita, porém, limitada.

A versão Comercial, que tem um curso de $760.

Também existe a ferramenta **CaseFile** que tem a função de analisar dados com a mesma flexibilidade dos gráficos do Maltego sem o uso de transformações.

É uma aplicação de inteligência visual que pode ser usado para determinar as relações e as ligações reais entre centenas de diferentes tipos de informações.

Você pode ligar pessoas e ações e suas ferramentas, vamos dar um exemplo:

Uma investigação criminal procura por traficantes, seus comparsas e sua hierarquia.

Com o **CaseFile,** você pode desenvolver e atribuir à investigação de modo gráfico toda a correlação entre eles.

**Na edição Community, você encontrará as seguintes limitações:**

* Máximo de 12 resultados por transform
* É necessário cadastro no site da PATERVA
* As chaves de API expiram a cada 2 dias
* Executado em um servidor mais lento, que é compartilhado entre todos os usuários da comunidade.
* A comunicação entre cliente e servidor não é criptografada.
* Não possui atualização, até a próxima versão principal
* Não há suporte para usuários
* Só poderá efetuar a varredura partindo dos servidores da Paterva Online
* Você não consegue exportar seu projeto para outras extensões.

A função do Maltego é exercer um “data mining”, ou na melhor tradução, podemos dizer que ele faz um “garimpo de informações”.

A maior parte das atividades do Maltego poderiam ser realizadas a partir de scripts, buscas na web, consulta de DNS, etc.

O Maltego não explora diretamente nenhuma vulnerabilidade do objeto alvo de pesquisa. Sendo assim, podemos considerar que ele realiza varreduras não intrusivas, ou como costumamos chamar; varreduras passivas.

Não adianta utilizar esta ferramenta se você não traçar um objetivo ou linha de pesquisa, ou, seja não ter um alvo específico ou apenas procurar por pontos de falhas.

Será melhor aplicado se você obtiver um alvo, onde, nesse alvo, você explorar ou tentar explorar as pesquisas previamente adquiridas com a ferramenta.

**Transform**: Devem ser pensados como pequenos pedaços de código com o objetivo de auxiliar o Maltego na sua mineração de dados.

Esses códigos podem se alterados para melhor apoia-lo em sua pesquisa, são geralmente desenvolvidos em Python ou PHP.

**TDS(Transform Distribution Server):** É uma aplicação web que permite a distribuição e gestão de transformações, seeds e configurações. Essencialmente, o TDS significa que suas transformações são escritas como um serviço WEB (ou aplicações/páginas), e a TDS chamará esses scripts.

Você pode obter acesso às TDSs através do link <https://cetas.paterva.com/TDS/>

As TDSs podem ser públicas ou pagas, e por motivos óbvios, as melhores e úteis são as pagas.

**Varreduras Intrusivas**

Nmap é um software livre que realiza port scan desenvolvido pelo Gordon Lyon, auto proclamado hacker “Fyodor”. É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.

É conhecido pela sua rapidez e pelas opções que dispõe.

O Nmap é um programa CUI (Console User Interface), pelo que corre na linha de comandos, mas este tem uma interface gráfica (GUI), o NmapFE (Nmap Front End), que foi substituído pelo Zenmap em 11 de Outubro de 2007, por ser uma versão portátil e prover uma interface melhor para execução e especialmente para visualização e análise dos resultados do Nmap.

**Quando um firewall identifica que determinada requisições estão passando por portas que não deveriam passar como a 135(Windows) e vem de portas altas acima de 1024 então isso pode ser uma varredura então firewall vai lá e te bloqueia**

**Comandos nmap**

**nmap -sV:** Faz varredura e traz também o versionamento do alvo.

**nmap -p1 “porta” -sV:**

**nmap -O:** Faz varredura e descobre qual sistema operacional da máquina que foi usada como parâmetro.

**nmap -A:** Faz varredura avançada e descobre máximo de informações possíveis.

**nmap -sS:**

**nmap -R:**

**nmap -135:** Faz varredura e descobre se maquina pesquisa utiliza ou não sistema operacional Windows.

**nmap -sU:** Faz varredura aos serviços que utilizam o protocolo UDP.

**nmap -T0 - 5:** Faz varredura de acordo com a velocidade que foi colocada mais quanto menos tempo varredura menor número de informações coletadas.

**nmap -v:** Modo verbouse traz na tela tudo o que nmap esta fazendo importante para se saber se nmap esta travado ou ainda fazendo varredura, esta varredura pode ser melhorada acrescentando um “v”.

**nmap -F:** Fast mode escaneia menos portas por padrão ele vai diretamente nas portas mais conhecidas consequentemente ele acaba fazendo busca mais rápidas.

**nmap --open:** Faz varredura em somente portas que estão abertas ou possivelmente abertas.

**nmap --iflist:** Mostra dados da interface.

**nmap -iL”Nome pasta”**: Realiza a varredura sobre uma lista.

**nmap -iR”N”:** realiza varredura para procurar “N” IPs aleatórios e vai tentar fazer varredura nesses IPs

**nmap --exclude”---”:** Faz varredura de toda a rede exceto a citada.

**nmap --excludefile “nome pasta”:** Realiza a varredura na rede exceto as que estão citadas na pasta.

**nmap --dns-server “endereço”:** servidor DNS realiza a varredura.

**nmap -sV --version-intensity 0-9:** Controla a intensidade de busca sobre versionamentos

**nmap --send -ip:** Invez de mandar protocolo ARP manda protocolo IP.

**nmap --privileged:** Mostra que você tem permissão para realizar a varredura.

**nmap --traceroute:** Faz a varredura e mostra caminho em que ele percorreu.

**Relatórios Nmap**

**nmap -oN “Nome\_relatório” “site/IP”:** Realiza relatório normal sobre o pesquisado.

**nmap -oX “Nome\_relatório” “site/IP”:** Gera relatório formato XML.

**nmap -oS “Nome\_SK” “site/IP”:** Gera relatório com uma letra maiuscula e uma minúscula.

**nmap -oG “Nome\_grepado” “site/IP”:** Realiza um relatório grepado que é separado por greps que faz fácil localização.

**Protocolo SCTP**

O protocolo SCTP é um protocolo de transporte confiável que opera sobre um serviço de pacotes não confiável e sem conexão, como é o caso do IP. O SCTP oferece a transferência de datagramas(mensagens) livre de erros e de duplicações através do reconhecimento transmissões (ACKs). A detecção de corrupção, perda e duplicação de dados é obtida através de mecanismo de checksum e número sequencias. Um mecanismo de retransmissão seletiva é usada para corrigir a perda ou a corrupção de dados.

**Protocolo ICMP**

ICMP, sigla para o inglês **Internet Control Message Protocol**, é um protocolo integrante do protocolo IP, definido pela RFC 792, e utilizado para fornecer relatórios de erros à fonte original. Qualquer computador que utilize IP precisa aceitar as mensagens IMCP e alterar o seu comportamento de acordo com o erro relatado. Os gateways devem estar programados para enviar mensagens ICMP quando receberem datagramas que provoquem algum erro.

**Tipos de Tramas do protocolo ICMP**

* **Echo Request/ Reply -** Mensagens para funções de teste e controle da rede, caso a maquina esteja ligada ira responder com um reply e se estiver inalcançavel request; Usadas pelo comando PING.
* **Destination Unreachable -** Enviado por um router que deixa fora um Datagrama; Tipo de mensagem que é obtida quando não se consegue localizar o equipamento alvo; (nem todos os datagramas perdidos são detectados)
* **CODE -** Indica a razão da perda do datagrama.
* **Timestamp Request / Reply -** Mensagens para sincronização dos relógios das máquinas.

**-PN** - Não realizar PING.

**-PS** - Scan utilizando o protocolo TCP/SYN.

-**PA -** Scan utilizando o protocolo TCP/ACK.

**-PU** - Scan utilizando o protocolo UDP.

**-PY** - Scan utilizando o protocolo SCTP.

**-PE** - Scan utilizando o protocolo ICMP Echo.

**-PP** - Scan utilizando o protocolo ICMP Timestamp.

**-PO** - Scan utilizando o protocolo IP/Ping.

**-PR** - Scan utilizando o protocolo ARP/Ping.

**Exemplo:** nmap -PR [www.laboratoriohacker.com.br](http://www.laboratoriohacker.com.br)

nmap -F -O ......... |grep “Running:” > /tmp/os;echo “$(cat /tmp/os |grep Linux |wc -l).....”

**Varreduras Intrusivas: Nmap**

Para todos aqueles que estão estudando sobre teste de penetração, exploiting, invasão de sistemas e tudo que está relacionado ao genero de segurança e afins. Esta é a maquina sagrada onde podem testar os seus estudos e aplica-los de forma prática.

Desenvolvida pela equipe do Metasploit a máquina virtual Metasploitable foi feita intencionalmente vulnerável para todos os tipos imagináveis de falhas de segurança poderem ser explorados, incentivando assim os estudos e ajudando na obtenção de novos conhecimentos para pentesters iniciantes.

A Metasploitable pode ser usada em treinamentos de cursos académicos ou particulares, e é compatível com VMWare, VirtualBox ou VMFusion. O login e senha padrão é **msfadmin**.

Você pode baixar a máquina virtual no endereço: <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

**NSE - Nmap Scripting Engine**

O NSE é distribuído com Nmap, junto com um conjunto de scripts maior a cada nova versão, e pode ser obtido através do site oficial. Informações adicionais às apresentadas nesta apresentação podem ser encontradas na documentação oficial do Nmap e do NSE, no portal NSEDoc de referência do NSE ou no livro de autoria do próprio Fyodor dedicado à ferramenta, que inclusive tem uma versão traduzida em português (PT-BR). Parte deste livro está disponível gratuitamente na internet para leitura e consulta. Vale mencionar que o capítulo do livro referente ao NSE faz parte do conteúdo disponibilizado neste treinamento.

Site: Descrição dos Scripts

<http://nmap.org/nsedoc/>

Os scripts são desenvolvidos em uma linguagem de script chamada LUA, que foi criada pelos alunos da PUC do Rio de Janeiro

**Nmap - Script Engine**

Os scripts disponibilizados pelo NSE são classificados quanto às categorias e ao tipo. As categorias dizem respeito à natureza da funcionalidade desempenhada e os tipos e a fase da varredura em que devem ser executadas, isto é, as categorias classificam os scripts pelo que eles fazem e os tipos, pelo momento em que o mesmo são executados durante uma varredura.

A listagem abaixo descreve cada categoria:

* auth -> Relacionados à mecanismos de autenticação e credenciais de acesso;
* broadcast -> Fazem descoberta de hosts não listados como alvos através do envio de pacotes broadcast;
* brute -> Visam descobrir credenciais de acesso através de ataques dicionário;
* default -> É a categoria padrão, em que os scripts devem fornecer respostas rápidas, concisas e confiáveis, além de serem pouco intrusivos, de fornecerem informações úteis para a maior parte dos usuários e de não estressarem o alvo a ponto de ser detectado por seus administradores como um ataque.
* discovery -> Visam descobrir ativamente mais informações sobre o alvo;
* dos -> Tentam causar indisponibilidade do alvo, ao provocar erros no lado do servidor;
* exploit -> Exploram uma dada vulnerabilidade conhecida;
* external -> Fazem consultas legitimas a recursos de terceiros, não listados como alvos;
* fuzzer -> Enviam pacotes contendo aleatórios ou inesperados pela aplicação servidor visando descobrir bugs e vulnerabilidades;
* intrusive -> Representam considerável risco de provocar erros no lado do servidor, utilizar uma quantidade significativa de recurso ou estressar o alvo a ponto de ser detectado por seus administrados como um ataque;
* malware -> Detectam remotamente se o alvo está infectado com um dado malware;
* safe -> Representam pouco risco e não devem causar erros no lado do servidor, utilizar muitos recursos ou explorar brechas de segurança;
* version -> Estendem a funcionalidade de detecção de versão do Nmap;
* vuln -> Verificam se há uma dada vulnerabilidade conhecida no alvo;

**O protocolo HTTP - Conceito**

O Hypertext Transfer Protocol (HTTP), em português Protocolo de Transferência de Hipertexto, é um produto de comunicação (na camada de aplicação segundo o modelo OSI) utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da World Wide Web.

Hipertexto é o texto estruturado que utiliza ligações lógicas (hiperlinks) entre nós contendo texto. O HTTP é o protocolo para a troca ou transferência de hipertexto.

Uma sessão HTTP é uma sequência de transações lógicas de rede de requisição-resposta. Um cliente HTTP inicia requisição estabelecendo uma conexão Transmission Control Protocol (TCP) para uma porta particular de um servidor (normalmente a porta 80).

Um servidor HTTP ouvindo naquela porta espera por uma mensagem de requisição de cliente. Recebendo a requisição, o servidor retorna uma linha de estado, como “HTTP/1.1 200 OK”, e uma mensagem particular própria. O corpo desta mensagem normalmente é o recurso solicitado, apesar de uma mensagem de erro ou outra informação também pode ser retornada.

**Métodos**

O protocolo HTTP define oito métodos (GET, HEAD, POST,PUT, DELETE, TRACE, OPTIONS e CONNECT) que indicam a ação a ser realizada no recurso especificado.

O método determina o que o servidor deve fazer com o URL fornecido no momento da requisição de um recurso. Um servidor HTTP deve implementar ao menos os métodos GET e HEAD.

**Método GET -** Solicita algum recurso como um arquivo ou um script CGI (qualquer que estiver identificado pelo URI) por meio do protocolo HTTP, por exemplo segue abaixo uma comunicação entre um cliente e um servidor HTTP. O servidor possui a URL [www.exemplo.com](http://www.exemplo.com), porta 80.

O pedido do cliente: GET/index.html HTTP/1.1

Host: [www.exemplo.com](http://www.exemplo.com)

O cabeçalho Host reconhece vários diferentes nomes DNS que tenham o mesmo IP.

A resposta do servidor: HTTP/1.1 200 OK

Date: Mon, 23 May 2005 22:38:34 GMT

Server: Apache/1.3.27 (Unix) (Red-Hat/Linux)

Last-Modified: Wed, 08 Jan 2003 23:11:55 GMT

Etag: “3f80f-1b6-3e1cb03b”

Accept-Rangers: bytes

Content-Lenght: 438

Connection: close

Content-Type: text/html; charset=UTF-8

**Método HEAD** - Variação do GET em que o recurso não é retornado. É usado para obter informações por meio do cabeçalho da resposta, sem ter que recuperar todo o conteúdo.

**Método POST** - Envia dados para serem processados (por exemplo, dados de um formulário HTML) para o recurso especificado. Os dados são incluídos no corpo do comando. Sua utilização em uma requisição ocorre quando é necessário enviar dados ao servidor para serem processados, geralmente por um programa script identificado no Request-URI. Uma requisição por meio desse método sempre requer que as informações submetidas sejam incluídas no corpo da mensagem e formatadas como uma query string, além de conter cabeçalhos adicionais especificados seu tamanho (Content-Lenght) e seu formato (Content-Type). Por isso, esse método oferece uma maior segurança em relação aos dados transferidos, ao contrário do método GET que os dados são anexados a URL, ficando visíveis ao usuário.

Por exemplo: POST/index.html HTTP/1.0

Accept: text/html

If-modified-since: Sat, 29 Oct 1999 19:43:31 GMT

Content-Type: application/x-www-formurlencoded

Content-Lenght: 41

Nome=NomePesssoa&Idade=99Curso=Computação

**Método PUT** - Envia certo recurso.

**Método Delete** - Exclui o recurso.

**Método Trace** - Ecoa o pedido, de maneira que o cliente possa saber o que os servidores intermediários estão mudando em seu pedido.

**Método Options** - Recupera os métodos HTTP que o servidor aceita.

**Método Connect** - Serve para uso com um proxy que possa se tornar um túnel SSL (um túnel pode ser usado, por exemplo, para criar uma conexão segura).

**Wordpress**

WordPress é um aplicativo de sistema de gerenciamento de conteúdo para web, escrito em PHP com banco de dados MySQL, voltado principalmente para a criação de blogs via web.

Essa é uma das ferramentas mais famosas na criação de blogs disputando diretamente com o serviço do Google chamado Blogger. No entanto, o WordPress é adotado por aqueles que queiram um blog mais profissional e com maiores recursos diferenciais.

O WordPress é utilizado também como plataforma de desenvolvimento de sites de comércio eletrónico, revistas, jornais, portfólios, gerenciador de projeto, diretório de eventos e outros conteúdos devido a sua capacidade de extensão através de plugins, temas e programação PHP.

**Joomla**

Joomla! é um dos principais sistemas de gestão de conteúdo da atualidade (Content Management System - CMS).

A separação entre design, programação e conteúdo permite uma grande flexibilidade na produção de sites com design extremamente customizados.

Além disso, existem milhares de templates prontos que agilizam o processo de criação de sites com rapidez e menor investimento.

O Joomla! é utilizado para o desenvolvimento de lojas virtuais, blogs, revistas online, portais de conteúdo, jornais, catálogos de produtos/serviços outros formatos de conteúdo.

Isso é possível devido à grande diversidade de extensões - 10 .071 mil - que permitem agregar novas funcionalidades com rapidez e eficiência.

Possui versões em 64 idiomas e 2,4% dos sites da internet utilizam o Joomla!.

É desenvolvido em PHP e pode ser executado no servidor Web Apache ou IIS e base de dados MySQL.

**Achar plugins**

Nmap --scripthttp-wordpress-plugins --script-argshttp-wordpress-plugins.root=/wordpress/,http-wordpress-plugins-search=100 www.google.com

**Brute Force - WordPress**

nmap --script http-wordpress-brute --script-args userdb=usuario.txt, passdb=senhas.txt,http-wordpress-brute.threads=10,http-wordpress.brute.uservar=username,http-wordpress.brute.passvar=password,http-wordpress-brute.uri=/wordpress/wp-login.php,brute.firstonly=true [www.google.com](http://www.google.com)

**Brute Force - Joomla**

nmap --script http-joomla-brute --script-args userdb=usuario.txt, passdb=senhas.txt,http-joomla-brute.threads=10,http-joomla.brute.uservar=username,http-joomla.brute.passvar=password,http-joomla-brute.uri=/administrator/index.php,brute.firstonly=true [www.google.com](http://www.google.com)

**MySQL**

O MySQL é um sistema de gerenciamento de banco de dados (SGBD), que utiliza a linguagem SQL (Linguagem de Consulta Estruturada, do inglês Structured Query Language) como interface. É atualmente um dos bancos de dados mais populares, com mais de 10 milhões de instalações pelo mundo.

Entre os usuários do banco de dados MySQL estão: NASA, Friendster, Banco Bradesco, Dataprev, HP, Nokia, Sony, Lufthansa, U.S.Army, U.S.Federal Reserve Bank, Associated Press, Alcatel, Slashdot, Cisco Systems, Google e outros.

**Brute Force - MySQL**

nmap -p3306 --script mysql-brute --script-args userdb=usuario.txt,passwd=usuario.txt,brute.firstonly=true,unpwdb.timelimit=0 10.50.0.26

nmap --script mysql-database --script-args mysqluser=usuario,mysqlpass=senha 10.50.0.26

nmap --script mysql-users --script-args mysqluser=usuario,mysqlpass=senha 10.50.0.26

nmap --script mysql-variables --script-args mysqluser=usuario,mysqlpass=senha 10.50.0.26

nmap --script mysql-empty-password

**Evasão com Nmap**

Muitas vezes, administradores de sistemas de redes, instalam e configuram dispositivos de proteção em seus ambientes, afins de proteger suas empresas de ataques.

A falta de conhecimento nas técnicas de invasão ou o hábito de considerar que ninguém irá descobrir determinadas brechas de segurança, fazem com que as empresas sejam prejudicadas.

O objetivo desta aula é apresentar algumas técnicas de Evasão com o Nmap, afim de enganar os dispositivos de segurança ou dificultar a sua identificação.

**Fragmentação de Pacotes**

nmap -f [www.google.com](http://www.google.com)

**Quebra de Pacote**

nmap --mtu 32 [www.google.com](http://www.google.com)

**Aumenta a quantidade de bits**

nmap --data-lenght “Nº” [www.google.com](http://www.google.com)

**Ataca e inventa IP culpado**

nmap -D [www.google.com](http://www.google.com)

nmap -D RND:5 [www.google.com](http://www.google.com)

**Rastreia IP**

nmap -e eth0 -Pn -S IP atacante IP Alvo

**Seleciona porta de saída e chegada**

nmap -g53 -p135 [www.google.com](http://www.google.com) g=porta de saída, p=porta de chegada.

**Checagem de pacotes badsum**

nmap --badsum [www.google.com](http://www.google.com)

**Burlar IDS**

nmap --randomize-hosts 10.50.0.1/24

**Descoberta de geolocalização**

nmap --script ip-geolocation-geoplugin [www.google.com](http://www.google.com)

**Altera MAC**

nmap --spoof-mac Dell [www.google.com](http://www.google.com)

**Senhas Padronizadas**

Em diversas empresas, há uma pressão natural para entregar sistemas e conectividades em um curto intervalo de tempo.

Além disso, administradores de sistemas não criam o hábito de proteger seu ambiente, mantendo senhas fracas ou até mesmo, senhas padrão.

Quando trabalhamos em processo de auditoria em segurança da informação, é natural que testemos as principais senhas em sistemas e dispositivos conectados a rede.

Para facilitar esse processo, alguns sites disponibilizam uma lista de senhas padronizadas, separadas por dispositivos e versões:

Sites: <http://routerpasswords.com/>

<http://www.phenoelit.org/dpl/dpl.html>

<https://www.cirt.net/passwords>

**Shodan**

O Shodan é um motor de busca que não dá as respostas comuns de uma pesquisa, mas que poderá dar acesso a tudo o que esteja ligado à rede.

Enquanto o Google pesquisa por websites, o Shodan procura por servidores, webcams, routers ou impressoras. Mas isso não fica por aqui: pode localizar e permitir acesso a qualquer dispositivo ligado à rede, como smartphones, IPhones ou mesmo eletrodomésticos. No total, são 500 milhões de dispositivos e serviços adicionados no banco de dados do Shodan.

Os utilizadores do Shodan conseguiram localizar os sistemas de controle de um parque aquático, um posto de gasolina, semáforos e até mesmo centrais nucleares e de um acelerador de partículas.

O motor de busca limita as pesquisas a realizarem 10 buscas sem contas e 50 buscas com conta.

Para ver tudo o que o Shodan consegue alcançar, é necessária muita burocracia e pagamento.

Os principais utilizadores do motor de busca são “penetration testers”, profissionais de segurança e investigadores académicos.

SHODAN interroga portas e pega os banners, resultando, então, os índices de banners (ao invés do conteúdo da web) para pesquisa.

Você pode acessa-lo pelo endereço: <http://www.shodanhq.com/>

**Comandos de Pesquisa**

port: nº da porta

after: dd/mm/aaaa

before: dd/mm/aaaa

os: Sistema operacional

country: Sigla país

net: Busca pelo IP

**Web Crawlers**

Web crawler, em português rastreador web, é um programa de computador que navega pela internet de uma forma metódica e automatizada. Outros termos para Web crawlers são indexados automáticos, bots, web spiders, Web robot, ou Web scutter.

O processo que um Web crawler executa é chamado de Web crawling ou spidering. Muitos sites, em particular os motores de busca, usam crawlers para manter uma base de dados atualizada.

Os Web crawlers são principalmente utilizados para criar uma cópia de todas as páginas visitadas para um pós-processamento por um motor de busca que irá indexar as páginas baixadas para prover buscas mais rápidas.

Crawlers também podem ser usadas para tarefas de manutenção automatizadas em um Web site, como checar os links ou validar o código HTML. Os crawlers também podem ser usadas para obter tipos específicos de informação das páginas da web, como minerar endereços de email (mais comumente para spam).

Um Web crawler é um tipo de robô de Internet ou agente de software.

Em geral, ele começa com uma lista de URLs para visitar (também chamado de seeds). À medida que o crawler visita essas URLs, ele identifica todos os links na página e os adiciona na lista de URLs para visitar. Tais URLs são visitadas recursivamente de acordo com um conjunto de regras.

**DirBuster**

DirBuster é uma aplicação feita em Java para descobrir nomes de diretórios e arquivos presentes em um site ou servidor usando brute force. Com isso, torna-se mais fácil a busca por algum diretório específico, facilitando a busca por dados ou diretórios que deveriam ser sigilosos.

O DirBuster tenta encontrar todos os diretórios e arquivos do site alvo.

No entanto, ferramentas dessa natureza são muitas vezes listadas com arquivos e diretórios comuns (padrões, exemplo: /admin/login.php).

DirBuster vem com um total de 9 listas diferentes, isto faz DirBuster extremamente eficaz para encontrar os arquivos e diretórios ocultos, ou que não seguem um padrão .

E se isso não fosse suficiente, DirBuster também tem a opção de realizar uma força bruta pura, o que deixa os diretórios e arquivos ocultos sem onde se esconder.

**O DirBuster oferece os seguintes recursos:**

* Multi-threaded é possível efetuar mais de 6.000 solicitações por segundo.
* Analisa sites HTTP e HTTPS.
* Verificar a existência de diretórios e arquivos.
* Capaz de executar uma lista de verificação de força bruta baseado em uma wordlist ou pura.
* DirBuster pode ser iniciado em qualquer diretório.
* Cabeçalhos HTTP personalizados podem ser adicionados.
* Suporte a proxy.
* Extensões de arquivos personalizados podem ser usados.
* O desempenho pode ser ajustado durante o programa em execução.
* Suporta Basic, Digest e NTLM auth.
* Pode ser executado por linha de comando ou interface gráfica.

O DirBuster vem com um conjunto de listas únicas de diretórios e arquivos, estas foram geradas com base no arquivo e diretório de nomes que sejam efetivamente utilizadas por desenvolvedores de sites da internet.

**Scanners de Vulnerabilidade**

Um Scanner de vulnerabilidade é um software que, dado um determinado alvo, seja ele um software, um computador ou um dispositivo de rede, irá analisa-lo em busca de vulnerabilidades existentes no alvo.

O scanner irá, sistematicamente, testar o alvo em busca de pontos vulneráveis a ataques (senhas padrão, serviços inseguros escutando em portas públicas , sistemas vulneráveis a falhas conhecidas, por exemplo).

Pode ser utilizado tanto para prevenção, na busca de falhas para correção, quanto para ataques, na identificação de vulnerabilidades acessíveis ao atacante.

**Busca padrão WordPress**

ruby wpscan.rb --url [www.example.com.br](http://www.example.com.br)

**Busca padrão Joomla**

joomscan -u [www.example.com.br](http://www.example.com.br)

**MBSA**

O