VARREDURA DE PORTAS COM NMAP

O Nmap é o padrão do mercado para scanning de portas, livros inteiros já foram escritos somente sobre o uso dessa ferramenta e a página de seu manual pode parecer um pouco desanimadora.

Discutiremos o básico sobre esse scanner de portas aqui e retornaremos a essa ferramenta nos próximos capítulos.

Os firewalls com sistema de prevenção e detecção de intrusão tem feito grandes progressos em detectar e bloquear tráfego de scanners, portanto pode ser que você execute um Scan com o Nmap e não obtenha resultado algum. Embora você possa ter sido contratado para executar um teste de invasão externo em uma faixa de endereço de rede sem hosts ativos, é mais provável que você esteja sendo bloqueado por algum firewall. Por outro lado, os resultados do seu Nmap podem informar que todos os hosts estão ativos e que estão ouvindo todas as portas caso seu scan não seja detectado.

SCAN SYN

Scan SYN é uma varredura que não finaliza o handshake TCP. Uma conexão TCP começa com um handshake de três vias (three way handshake) SYN > SYN-ACK > ACK.

Em um scan SYN o Nmap envia o SYN e espera pelo SYN-ACK caso a porta esteja aberta, entretanto não envia o ACK que completa a conexão.

Se o pacote SYN não receber nenhuma resposta SYN-ACK, a porta não está disponível, podendo estar fechada ou filtrada, dessa maneira o Nmap descobre se uma porta está aberta sem nem mesmo se conectar totalmente ao computador alvo. A sintaxe para um scan SYN é representada pela flag -sS (Case-sensitive).

```
root@kali:~#nmap -sS ENDEREÇO-IP
```

SCAN DE VERSÕES

Como o scan versões, o Nmap completa a conexão e em seguida tenta determinar quais softwares estão executando no sistema alvo (e se possível a versão) usando técnicas como o acesso aos banners.

Dessa vez obtivemos muito mais informações sobre os nossos alvos. Usaremos esse resultado para procurar potenciais vulnerabilidade nos próximos capítulos, tenha em mente que o Nmap pode informar a versão incorreta, (em alguns

casos por exemplo) se o software foi atualizado, porém o banner de boas-vindas não foi alterado como parte do path.

No mínimo seu scan de versões nos proporcionará um bom ponto de partida para novas pesquisas.

root@kali:~#nmap -sV ENDEREÇO-IP

SCANS UDP

Tanto os scans SYN quantos os scans de versão do Nmap são varreduras TCP que não fazem consultas em portas UDP.

Como o UDP não é orientado a conexão, a lógica do scanner é um pouco diferente. Em um scan UDP o Nmap envia um pacote UDP a uma porta, de acordo com a porta, o pacote enviado é específico de um protocolo.

Se uma resposta foi recebida, a porta será considerada aberta, se a porta estiver fechada o Nmap receberá uma mensagem de porta inacessível do ICMP. Se o Nmap não receber nenhuma resposta então a porta estará aberta e o programa que estiver ouvindo não responde a consulta do Nmap ou o tráfego está sendo filtrado.

Desse modo o Nmap nem sempre é capaz de fazer distinção entre uma porta UDP aberta e uma que esteja sendo filtrada por um firewall.

root@kali:~#nmap -sU ENDEREÇO-IP

OUTROS SCANS

root@kali:~# nmap 127.0.0.1 => scan básico.

root@kali:~# nmap -sP [ip] => scan usando somente ping.

root@kali:~# nmap -P0 [ip] => força o scan mesmo sem resposta por ping.

root@kali:~# nmap -PR [ip] => "ping" usando ARP (mais rápido em rede).

root@kali:~# nmap -F [ip] => portas mais comuns.

root@kali:~# nmap -O [ip] => tenta detectar SO.

root@kali:~# nmap -sV [ip] => detecção de serviços e versões (grab banner).

TÉCNICAS DE EVASÃO

root@kali:~# nmap -D [ipFake],[ipFake] [ip] => Decoy fake scan

root@kali:~# nmap -g 53 [ip] => scan através da porta DNS (evade firewalls)

root@kali:~# nmap -T [0-5] [ip] => diminui performance, evita flood

root@kali:~# nmap -f [ip] => fragmenta os pacotes

https://www.youtube.com/watch?v=oqgg6qxaowq

https://www.tenable.com/blog/getting-started-with-nessus-on-kali-linux

NESSUS, SCANNER DE VULNERABILIDADES

O Nessus é um dos scanners de vulnerabilidade comerciais mais utilizados por pentesters e analistas de segurança, embora muitos fornecedores possuam produtos comparáveis.

O Nessus compartilha seu nome com um centauro que foi morto pelo herói mitológico grego Héracles. O banco de dados do Nessus incluí vulnerabilidades em plataformas e protocolos. O seu scanner realiza uma série de verificações para detectar problemas conhecidos, você encontrará capítulos de cursos e livros dedicados exclusivamente ao Nessus.

A medida que se familiarizar com a ferramenta você descobrirá o que funciona melhor em seu caso. O Nessus está disponível nas formas de versão profissional (paga), que os pentesters e equipes internas de segurança podem usar para efetuar scans em busca de vulnerabilidades, todavia você pode usar a versão gratuita não comercial chamada nessus home para executar os exercícios propostos no curso.

O Nessus home está limitado a efetuar a varredura de 16 endereço IP, o software não está pré-instalado no Kali porém a instalação dele foi abordada em capítulos anteriores desse curso.

Antes de executar o Nessus é necessário iniciar o daemon do software, para isso digite o comando service como mostrado aqui para iniciar a interface web na porta TCP 8834.

root@kali:~#service nessusd start

Agora abra o navegador web e acesse **https://kali:8834** ou **https://SEU-IP:8834**

Depois de alguns minutos de inicialização você deverá ver uma tela de login, utilize as credenciais de login criadas e efetue o registro no site caso ainda não tenha feito.

Para criar uma nova política, click em "nova política" a esquerda da interface do Nessus.

O assistente de política do Nessus ajudará a criar uma política que seja produtiva para os objetivos do seu scan, para o nosso exemplo selecione scan básico de rede, agora você deve fornecer algumas informações sobre a política.

Inclua um nome, uma descrição e indique se outro usuário do Nessus pode acessar essa política. Depois de concluído, clique em próximo, uma pergunta será feita para saber se esse é um scan interno ou externo, selecione interno e clique em próximo.

Se houverem credenciais de acesso, o Nessus pode autenticar-se junto aos hosts e procurar vulnerabilidades não aparentes do ponto de vista da rede. Esse recurso é frequentemente usado por equipes internas para testar a postura de suas redes quanto à segurança.

Agora vamos alterar para a aba "Scans" e executar o Nessus em nossa máquina alvo.

Clique em "Scan > Novo Scan" e preencha as informações, o Nessus deve saber o nome, política e em quais sistemas deverá executar o scan.

O Nessus executa uma série de sondagens no alvo em uma tentativa de detectar ou de excluir o máximo possível de problemas. O scan em execução é adicionado à aba "Scans", depois de concluído, clique nele para visualizar os resultados.

NMAP SCRIPTING ENGINE

Assim como Metasploit evoluiu a partir de um framework de exploração de falhas até se tornar um pacote completo de testes de invasão com centenas de módulos, o Nmap de modo semelhante evoluiu além do seu objetivo inicial que era o de efetuar scanning de portas.

O **Nmap Script Engine (NSE)** permite executar scripts publicamente disponíveis e possibilita a criação dos seus próprios scripts. Você encontrará os scripts empacotados com o **NSE** no Kali em **/usr/share/nmap/scripts** os scripts disponíveis se enquadram em diversas categorias, incluindo

coleta de informação, avaliação ativa de vulnerabilidades, pesquisa de sinais de comprometimentos anteriores, entre outros.

O comando:

```
root@kali:~# nmap -sC ENDEREÇO-IP
```

Executa todos os scripts da categoria default, podemos obter uma série de informações úteis que extrapolam o uso padrão do Nmap.

Outro exemplo do uso de scripts, desta vez um que não faz parte do conjunto default.

A partir de nosso uso básico do Nmap no capítulo anterior, sabemos que nosso alvo Linux está executando o NFS Network file System.

O NFS permite que computadores clientes acessem arquivos locais por meio da rede, porém em sua carreira na área de testes de invasão você verá que quando se trata de configurar o NFS de forma segura, é mais fácil falar do que fazer.

Muitos usuários não pensam nas consequências de dar acesso aos seus arquivos no que diz respeito à segurança. O script **nfs-ls.nse** se conectará com o NFS e fará auditoria dos compartilhamentos. Podemos ver mais informações sobre um script por meio do comando **--script-help**.

```
root@kali:~# nmap --script-help nfs-ls
```

Esse script monta os compartilhamentos remotos, faz uma auditoria de suas permissões e lista os arquivos incluídos no compartilhamento. Use o comando abaixo para lançar o script:

```
root@kali:~# nmap --script=nfs-ls ENDEREÇO-IP
```

O script do NSE encontrou um compartilhamento NFS em **/export/georgia** em um sistema operacional Linux.

Observe que o diretório **.ssh** listado pode conter informações críticas acerca do sistema, como chaves SSH e (caso a autenticação com chave pública seja permitida pelo servidor) uma lista de chaves autorizadas.

Esse erro de controle no acesso traz um efeito interessante ao nosso teste de invasão, sabendo que o diretório possui permissão de escrita, podemos adicionar uma nova chave SSH à lista **authorized_keys** (uma chave nossa).

Observe que um erro aparentemente insignificante que possibilitava a edição de documentos em pastas compartilhadas se transforma na capacidade de fazer login no sistema remoto e executar comandos (uma autêntica invasão do sistema). Essa tentativa de invasão será abordada no capítulo pertinente.

O Nmap foi executado tendo como alvo uma máquina virtual linux ubuntu 8.10 que pertence ao conjunto de exemplos do livro **Testes de Invasão:** Uma introdução prática ao hacking (Georgia Weidman). Algumas atividades práticas desse curso serão retiradas do livro supracitado.

Recomenda-se ao aluno que siga as instruções do link: https://www.amazon.com.br/Testes-invas%C3%A3o-introdu%C3%A7%C3%A3o-pr%C3%A1tica-hacking-ebook/dp/B06Y3H7NLY#reader_B06Y3H7NLY

Podendo baixar as máquinas virtuais citadas no fragmento do livro em: https://nostarch.com/download/Penetration%20Testing%20Georgia%20Weidman%20Supplementary%20Files%20No%20Starch%20Press%20[mininova].torrent

METASPLOIT, MÓDULO SCANNER

O Metasploit também pode conduzir varreduras de vulnerabilidade utilizando seus vários módulos auxiliares. Esses módulos não nos permitem o controle do computador-alvo, entretanto nos ajudarão a identificar vulnerabilidades posteriormente exploráveis.

Um desses módulos do Metasploit procura serviços FTP que permitem acesso anônimo. Apesar da facilidade em tentar um login anônimo manualmente, o Metasploit automatiza o processo em vários hosts economizando tempo em ambientes extensos.

Utilizamos o comando **use** para selecionar um módulo em particular, em seguida o comando **set** defini o alvo, finalmente o comando **exploit** executa a varredura.

Lembre-se que para iniciar o Metasploit deve-se digitar **msfconsole** no terminal:

```
msf > use scanner/ftp/anonymous

msf auxiliary(anonymous) > set RHOST ENDEREÇO-IP

msf auxiliary(anonymous) > exploit
```

Existem diversos módulos auxiliares no Metasploit, cabe a você pesquisar quais são e como utilizá-los.

NIKTO, SCANNING DE APLICAÇÕES WEB

O seu alvo também pode ter aplicações web prontas e instaladas, como aplicações para folha de pagamento, Webmail e outras que podem ser vulneráveis. Se encontrarmos uma instância de software que sabemos ser vulnerável, poderemos explorá-lo para adentrar um sistema remoto.

Problemas de aplicações web são particularmente interessantes em muitos testes de invasão externos em que a sua superfície de ataque poderá estar limitada a pouco mais do que os servidores web.

Por exemplo, como você pode ver ao navegar para a página Web default, um servidor web em nosso alvo Linux revela uma página default do Apache, ao menos que possamos descobrir uma vulnerabilidade no software subjacente do servidor web, teremos dificuldade em explorar uma página simples que exiba apenas "It works!".

Vamos usar um web scanner para procurar páginas adicionais que podem não estar sendo vistas.

O Nikto é um scanner de vulnerabilidade de aplicações web presente no Kali Linux. Sua função é semelhante ao Nessus, entretanto específico para aplicações web, ele procura problemas como arquivos perigosos, versões desatualizadas e erros de configuração.

Para executar o Nikto em nosso alvo Linux informaremos o host em que faremos scan por meio da flag **-h**.

```
root@kali:~# nikto -h ENDEREÇO-IP
```

Observe que ao fazer a varredura diversas informações são apresentadas pelo **Nikto**, uma delas (particularmente interessante) é a presença de uma versão vulnerável do software **TikiWiki** no servidor Linux.

Outra informação importante apresentada pelo **Nikto** é a possibilidade do alvo portar uma vulnerabilidade no **TikiWiki** (**OSVDB-40478**). Ao pesquisar essa vulnerabilidade (**OSVDB-40478**) concluímos que essa vulnerabilidade possui um exploit associado no **Metasploit** framework, que poderá ser usado durante a etapa de exploração de falhas.

Atenção, é importante ler bem as informações retornadas pelo software, visto que o terminal do Linux não organiza informações de maneira tão amigável.

Teste o **Nikto**, utilizando a máquina virtual Ubuntu disponibilizada anteriormente. Você pode testar em sites seus, ou em sites de terceiros com autorização prévia do administrador.

CREDENCIAIS DEFAULT NO XAMPP 1.7.2

Ao navegar para o nosso servidor web no Windows XP vemos que em **http://192.168.1.106** (endereço IP do Windows XP alvo) a página Web default se anuncia como **XAMPP 1.7.2.**

Por padrão instalações do XAMPP incluem o phpmyadmin que é uma aplicação web para administração de banco de dados. Em uma situação ideal o phpmyadmin não estaria disponível por meio da rede, ou pelo menos, deveria exigir credenciais para que pudesse ser acessado. Todavia nessa versão do XAMPP a instalação do phpmyadmin em **http://192.168.1.106/phpmyadmin/** está disponível e aberta.

O phpmyadmin nos dá acesso de **root** no mesmo servidor MySQL com o qual segundo nos informou o **NSE** não seria possível estabelecer conexão.

Ao usar o phpmyadmin podemos ignorar essa restrição e executar queries SQL no servidor.

Além da inclusão do phpmyadmin, uma pesquisa no Google nos informa que o XAMPP 1.7.3 e versões mais antigas vêm com software **WebDAV** (Web Distributed Authoring and Versioning) usado para administrar arquivos em um servidor web por meio de HTTP.

A instalação do WebDAV no XAMPP tem nome de usuário e senha default iguais a **wampp:xampp** se esses valores não forem alterados, qualquer pessoa que tiver acesso ao WebDAV poderá fazer login, desfigurar o site e possivelmente efetuar o upload de scripts que permitirão que invasores consigam entrar no sistema por meio do servidor web.

Podemos usar a ferramenta **Cadaver** para interagir com um servidor WebDAV, usamos o Cadaver para tentar fazer uma conexão com o servidor WebDAV em **http://192.168.1.106** e testar o conjunto padrão de credenciais.

O login com o Cadaver foi bem-sucedido, nosso alvo Windows XP usa as credenciais default do WebDAV. Agora que

temos acesso ao serviço poderemos fazer o upload de arquivos no servidor web. Essa exploração será abordada em um capítulo pertinente.

EXPLORANDO PORTAS, ANÁLISE MANUAL

As vezes nenhuma solução chega perto da análise manual de vulnerabilidades para verificar se um serviço resultará em um comprometimento.

Não há melhor maneira de se aperfeiçoar a análise manual do que a prática. Iremos explorar algumas pistas interessantes obtidas pelo scanner de portas e de vulnerabilidades.

Uma porta que não apareceu em nosso scan automatizado foi a porta 3232, em nosso alvo Windows ao tentarmos efetuar a varredura dessa porta com scan de versões do Nmap perceberemos que haverá uma falha, esse comportamento sugere que o programa que está ouvindo foi projetado para compreender um dado de entrada em particular, logo tem dificuldade de processar qualquer outra informação.

Esse tipo de comportamento é interessante para os pentesters porque programas que falham ao lidar com dados de entrada indevidos não estão validando suas entradas de forma adequada.

A saída nos levou a acreditar que o software é um servidor web, é possível fazer conexão usando um navegador no endereço **http://192.168.1.106:3232.**

A página web disponibilizada não nos diz muito, todavia a partir daqui, podemos nos conectar manualmente usando o netcat. Sabemos que o software é um servidor web, portanto conversaremos com ele assumindo essa hipótese.

Podemos navegar para página web default, portanto podemos usar **GET / HTTP/1.1** para pedir a página default ao servidor web.

O servidor se anuncia como sendo o **Zervit 0.4.** O primeiro link ao efetuarmos uma pesquisa no Google em busca de **Zervit 0.4** é **"Zervit 0.4 exploit".**

Isso não é um bom sinal para o software, esse servidor web está sujeito a vários problemas de segurança que incluem um **buffer overflow** e uma vulnerabilidade de **inclusão de arquivo local**, que nos possibilita incluir outros arquivos no sistema.

Esse serviço é tão sensível que é melhor evitar ataques de buffer overflow pois um movimento em falso pode provocar uma falha e disponibilização do serviço.

A inclusão de arquivos locais por outro lado parece promissora, sabemos que o servidor pode processar solicitações **HTTP GET**. Como exemplo podemos fazer o download do arquivo **boot.ini** do Windows XP ao retrocedermos cinco níveis de diretório no drive **C:** usando **GET**.

Podemos acessar o **boot.ini**, arquivo de configuração que informa o Windows quais opções do sistema operacional devem ser exibidas no momento do boot, usaremos essa inclusão de arquivo local para obter outros arquivos sensíveis nos próximos capítulos do curso.

ENCONTRANDO USUÁRIOS VÁLIDOS NO SMTP

Podemos aumentar nossas chances de um ataque bem-sucedido de senhas se encontrarmos nomes válidos de usuários para os serviços. Uma maneira de descobrir nomes válidos de usuários em servidores de e-mail é o comando **VRFY SMTP**, caso ele esteja disponível.

Como sugerido pelo nome, **VRFY** verifica se um usuário existe. O **NSE** descobriu que o verbo **VRFY** está habilitado no alvo **Windows XP** anteriormente (você pode refazer o scan e olhar atentamente o retorno do software).

Conecte-se à porta **TCP 25** usando o **Netcat** e use **VRFY** para verificar nomes de usuários.

Ao usar o comando, percebemos que o usuário **georgia** é um nome válido, porém não há nenhum usuário chamado **john**. Posteriormente usaremos usuários previamente descobertos em um processo que busca adivinhar senhas.

Lembre-se que os comandos para essa interação são:

```
root@kali:~# nc ENDEREÇO-IP 25

VRFY georgia

VRFY john
```

https://securityonline.info/category/penetration-testing/network-pentest/vulnerability-analysis/