**ESQUEMA DE PLANO DE AULA PRÁTICA**

**Tarefa 3a** "Ferramentas de Aquisição de Informações"

Tópico no Moodle: Scanner de Portas **Nmap** ("Network Mapper")

Data: 12-04-2013  
  
Tempo de Aula: 2 horas-aula  
  
Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Aluno\_2> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ASSUNTO**

Utilização básica do scanner de portas NMAP (**Network Security Scanner**). **NMAP** é um scanner de segurança de rede, que varre portas, indicando se aberta, fechada ou filtrada, associados à portas TCP, numa máquina em uma rede, ou num segmento de uma rede (um grupo de máquinas).

O tópico é estudado de forma simplificada, mas Nmap ("Network Mapper") é utilitário com licença em software livre para descoberta de rede e auditoria de segurança em ambientes corporativos.

Situado numa máquina, pode verificar portas abertas em outra máquina em rede. Esta última, podendo ser o próprio “localhost”, uma máquina servidor ou um servidor Web que hospeda um *site*.

Numa forma mais profissional, o Nmap é considerado por muitos administradores de rede, como muito útil para tarefas como inventário de rede, gerenciar o escalonamento de *upgrade* de serviços e monitoramento de hosts.

O Nmap é um escaneador de hosts que usa recursos avançados para verificar o estado do seu alvo. A ferramenta é gratuita e encontrada nas versões Linux, Windows, Mac OS, Solaris, FreeBSD e OpenBSD. As versões para Windows e Linux contam com uma interface gráfica que facilitam a vida dos usuários. Aqui, analisaremos a versão para Linux, porém o funcionamento varia pouco em outros sistemas operacionais.

**BIBLIOGRAFIA BÁSICA**Página OpenVAS:[www.nmap.org](http://www.nmap.org) [http://www.insecure.org](http://www.insecure.org/)  
  
Links Importantes: http://www.youtube.com/watch?v=CTyvTqoQzzA

<http://www.slideshare.net/firebits/oficina-de-anlise-em-vulnerabilidades-openvas4-garoahc>

**OBJETIVOS DA AULA**

Conhecer um **scanner de portas**, quanto a seus resultados básicos:

1. Mostrar os resultados relativos às portas na forma Host-Porta-Serviço, quanto se está aberta ou fechada. Portas abertas indicam serviços ativos que podem ser atacados.

**SELEÇÃO DO CONTEÚDO – A PRÁTICA**

Um conteúdo mínimo, consistindo de um roteiro de aula, com o Nmap, visando o objetivo acima, pode ser colocada como:

Utilização do Nmap:

Apesar de existirem *front-ends* gráficos disponíveis, os comandos passados em modo texto (linha de comandos) permitem uma enorme flexibilidade e, ao contrário do que possa parecer, o uso não é difícil. A sintaxe do comando sempre será:

nmap [ <Scan Type> ...] [ <Options> ] { <target specification> }

Onde o (target) é o endereço IP do alvo (host) ou rede que se deseja escanear. Caso exista uma forma de resolver nomes, como um DNS configurado, você pode usar o nome do host ao invés do IP.   
  
Os parâmetros para <Scan Type> são ajustados de acordo com o que se deseja obter, os principais são:

-sT - Com esse parâmetro é feito um escaneamento através de tentativas de conexão TCP. Essa forma é muito fácil de ser identificada por firewalls e IDS;  
  
-sS – Assim, a tentativa será com pacotes TCP com a flag SYN ligada, ou seja, como apenas uma requisição de conexão. Essa técnica dificulta um pouco a detecção;  
  
-sP - Com essa opção o escaneamento será feito através de pacotes ICMP echo request. Verifica apenas se o host está ativo;  
  
-sU - Envia pacotes UDP com 0 byte para determinar o estado dessas portas;  
  
-sO - É usado para tentar determinar os protocolos suportados pelo host;  
  
-O - Com esse parâmetro é feito uma tentativa de determinar o sistema operacional de um host (no sentido de ser atacado).  
  
Com a opção -p podemos especificar portas ou faixas (ranges) de portas para análise.

**Estes são os principais parâmetros, e com eles podemos realizar os mais variados testes.**

**UTILIZANDO O NMAP**

**IDENTIFICANDO MÁQUINAS ATIVAS**

**Antes de tentar fazer um pentest, nós primeiro precisamos identificar as máquinas ativas que estão num domínio de rede alvo.**

**Um modo simples é usarmos um ping contra máquinas de uma rede alvo. Mas, isto pode ser rejeitado ou conhecido por um host, e nós não queremos assim.**

**Como fazer isto ...**

1. **Abra um terminal no seu Linux. Usando Nmap podemos descobrir se um host está ativo ou não. Isto é mostrado como segue:**

nmap -sP <ip\_do\_host>

**Execute um exemplo e veja a saída gerada pelo Nmap.**

1. **Descobrindo portas abertas:**

nmap <ip\_do\_host>

**Execute um exemplo e veja a saída gerada pelo Nmap.**

**Podemos também, explicitamente especificar um conjunto de portas para a varredura com o Nmap:**

nmap –p <porta\_inicial-porta\_final> <ip\_do\_host> **onde o hífen “-“ é do nmap.**

**Execute um exemplo e veja a saída gerada pelo Nmap.**

1. **Especificar Nmap para varrer a rede toda de uma organização numa determinada porta TCP:**

nmap -p <porta> <ip.ip.ip.\*>

**Por exemplo:** nmap –p 22 150.162.65.\* **(toda a rede da sala 1, onde 65 identifica a rede e ´\*´identifica qualquer máquina. Neste caso, a máscara usada é 255.255.255.0**

**Execute um exemplo e veja a saída gerada pelo Nmap.**

1. **Nmap tem uma interface gráfica chamada Zenmap, a qual pode ser invocada executando o comando zenmap numa janela de terminal.**

**Execute no prompt de comando: #** zenmap

1. **Fingerprint de Sistema Operacional**

**Qual SO está rodando numa máquina alvo ?**

**Neste ponto do processo de obter informação, devemos já ter documentado uma lista de endereços IP, máquinas ativas, portas abertas onde rodam serviços. A próxima etapa é determinar o sistema operacional da máquina ativa de interesse, no sentido de saber o tipo de sistema que estamos pretendendo o pentest.**

**Usando Nmap, emitimos o comando:**

nmap –O <ip\_do\_host\_alvo>

**Execute um exemplo e veja a resposta de saída do Nmap.**

1. **Fingerprint de um Serviço**

**Determinando os serviços rodando em portas específicas, garantimos um pentest bem sucedido numa rede alvo e podemos tirar quaisquer dúvidas resultantes na obtenção do fingerprint do OS.**

nmap -sV <ip\_do\_host\_alvo>

**Execute um exemplo e veja a resposta de saída do Nmap.**

**Deposite no Moodle, em nome de sua dupla, esta parte da tarefa dos seis itens acima. Para tal você pode pegar uma cópia deste texto e acrescentar suas respostas.**

**--------------------------------------------------------------------------------------------------------------------------**

**O artigo seguinte mostra outros exemplos:**

**(**Artigo Básico de [www.invasao.com.br](http://www.invasao.com.br/))

1. **Primeiro podemos testar com pacotes SYN, nas portas de 1 a 100, num roteador:**

nmap -sS 192.168.0.1 -p 1-100

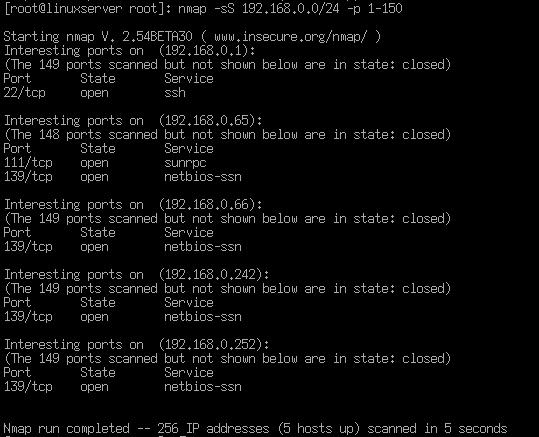
Uma resposta:



O que me mostra que tenho um serviço SSH (usado para acesso remoto) aberto na porta 22.

1. Podemos escanear um endereço de rede para determinar serviços ativos em mais de um host, basta para isso informar o endereço da rede, como no exemplo:

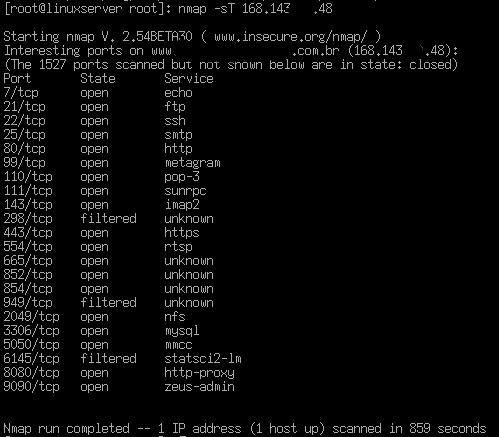
**nmap -sS 192.168.0.0/24 -p 1-150**



Os resultados são mostrados para todos os hosts da rede separadamente. Essa técnica é interessante pra identificar falhas de segurança em toda sua rede interna.

1. Agora tentaremos um alvo fora da minha rede interna. Tentaremos o IP 168.143.xx.48, omitiremos obviamente parte do endereço analisado.

**nmap -sT 168.143.xx.48**

  
  
Note que não especificamos um intervalo de portas, assim todas as portas serão escaneadas e nosso teste poderá demorar bastante dependendo do nosso link.

Aqui tentamos uma análise por tentativas de conexão TCP(opção -sT) ao invés de apenas envio de solicitações de conexão (opção -sS). É fácil observar que existem muitos serviços ativos e suas respectivas portas.

Tentaremos, agora, identificar o sistema operacional de um alvo em nossa rede local, para isso usaremos o parâmetro -O, assim:

**nmap -O 192.168.0.66**



Neste teste, o sistema operacional foi identificado como Windows, como pode ser visto na figura acima.

**Como se defender de um Scanner de Portas**

Utilitários como o Nmap estão em constante atualização, cada vez mais sutis, eles passam muitas vezes despercebidos por firewalls ou IDS. O que pode diminuir os riscos é a configuração de firewalls com regras bem definidas, diminuição dos serviços ativos no gateway deixando apenas aqueles indispensáveis ao seu funcionamento e análise constante de seus arquivos de log. Um sistema de detecção de intrusos, como o SNORT, é indicado também.

O Nmap pode e deve ser usado para averiguação do estado do seu host, principalmente se tratar de um servidor. Use, constantemente, para monitorar o estado das portas e se elas pertencem a algum serviço legitimo ou não.

Se um serviço não é legítimo, é porque existe um *“backdoor”* associado à porta, colocado por algum atacante, e isto significa uma ataque na forma de uma intrusão. Portas abertas podem significar *trojans* (Cavalos de Tróia) ou outras formas de programas de exploração de ataques instalados *(backdoor)*. Por isso, use também o programa **chkrootkit** para identificar mais facilmente essa tentativa de ataque. O **chkrootkit** pode ser encontrado no endereço <http://www.chkrootkit.org>.

**Conclusão:**

O Nmap pode ser considerado uma ferramenta Hacker/Cracker, ou um excelente utilitário para consultores de segurança e administradores de rede, o fato é que ele realiza de forma extremamente eficiente o que se propõe.

**--------------------------------------------------------------------------------------------------------------------------**

**MOSTRE OUTRO EXPERIMENTO (Deposite a tarefa no Moodle).**

Suas respostas, devem ser depositadas no prazo previsto pelo professor no sistema MOODLE, no link definido para tal, conforme os itens abaixo:

**Tarefa: A descoberta de hosts**

**Situação 1:** Suponha que você conheça um IP do alvo que deseja varrer em sua rede. No caso, este endereço IP pode ser, na rede virtual, 192.168.1.x onde x é:

113 – Backtrack,

254 – Ubuntu Server 11.10

116 – Windows Server 2008

117 – Metasploitable Linux

1. O escopo de sua tarefa (um localhost, um maquina física do LIICT, onde está seu colega, um servidor de Internet.
2. Realize a varredura simplesmente digitando o endereço alvo no campo Alvo da Inerface Zenmap.
3. Verifique as portas encontradas abertas. Indique o serviço associado.

**Situação 2:** Executando o número máximo de máquinas na rede que você puder, suponha que você desconheça o número de máquinas existentes na rede e os seus endereços IPs privados. Suponha que a rede é de sua propriedade e que não há risco nenhum em varrer a rede à procura de hosts ativos. Para isso, digite no campo comando do Zenmap:

nmap –sP –v 192.168.1.254/24.

Escreva o que observa como resposta.

**Situação 3:** Tome por base a situação 2, mas desta vez, suponha que a rede não é de sua propriedade e que você deve evitar ao máximo levantar suspeitas de que a rede está sendo varrida. Faça o teste varrendo a rede com a opção –PS, utilizando o comando:

nmap –PS 192.168.1.254/24.

Escreva o que observa como resposta.

**Situação 4:** Suponha que você queira descobrir os hosts da rede e você sabe que podem existir firewalls bloqueando o caminho. Caso os pacotes do Nmap encontrem um firewall, a resposta pode ser comprometida e não condizente com a realidade. Sabendo disto, você precisa maximizar as chances de obter bons resultados. Faça o teste com o comando:

nmap -PU -v <ip\_do\_host\_alvo>/<indicador de máscara>

Se você usar as VMs do seu Virtualbox, na máquina virtual do Windows Server 2008 tem um firewall que pode ser ativado/desativado. Escreva o que observa como resposta.

# Situação 5: Enganando um firewall

O NMAP também pode burlar os firewalls que são configurados para descartar os pedidos de conexões de outras redes, como já foi comentado no início. Para isso mudaremos a opção -D, que na verdade vai camuflar seu IP e com isso conseguiremos fazer nossa varredura. Usando essa opção associada com as outras temos uma das melhores buscas por portas possível.   
  
Essa opção será utilizada em conjunto com as outras vindo a frente das demais. Exemplo:   
  
**# nmap -sS 10.100.102.39 -D 10.100.102.113,200.192.35.6**

Onde:

* 10.100.102.39 é o IP o qual vou fazer a verificação.
* 10.100.102.113 é o meu IP.
* 200.192.35.6 é um IP qualquer que escolher para que camufle o meu IP.