Universidade da Beira Interior
Faculdade de Engenharia
Departamento de Informática

Segurança Informática
Guia para Aula Laboratorial 11
Licenciatura em Engenharia Informática
Licenciatura em Informática Web
Licenciatura em Tecnologias e Sistemas da Informação

Computer Security
Guide for Laboratory Class 11
Degree in Computer Science and Engineering
Degree in Web Informatics
Degree in Information Technologies and Systems

Sumário
Identificação de máquinas de rede, sistemas operativos e serviços em execução utilizando a ferramenta `nmap`. Exercícios de rastreio de endereços *Internet Protocol* (IP) e portos *Transmission Control Protocol* (TCP) e *User Datagram Protocol* (UDP). Breve utilização da ferramenta `tcpdump` para observar e capturar informação interessante que possa estar a fluir na rede.

Summary
Identification of network machines, operative systems and services provided using the `nmap` tool. Internet Protocol (IP) and Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port scanning exercises. Brief utilization of the `tcpdump` tool to observe and capture interesting information that may be flowing on the network.

Pré-requisitos:
Algumas tarefas deste guia laboratorial requerem a utilização das ferramentas `nmap`, `hping3` e `tcpdump`. Pressupõe-se o acesso a um sistema com estas ferramentas instaladas ou com privilégios para as instalar. Sugere-se o uso de uma distribuição Linux, para a qual existem implementações nativas e fáceis de instalar.

1 Rastreio de Endereços IP

IP Sweep (or Sweet?)

A fase que normalmente antecede o ataque aos sistemas de uma rede de computadores é aquela em que se identificam os sistemas (e endereços de rede) que estão ligados e que são potencialmente vulneráveis.

Tarefa 1 *Task 1*

Emita o comando `$ ip add` no terminal e analise o seu *output*. **Q1.: Qual é o endereço IPv4 do seu computador?**

O endereço é _____ . _____ . _____ . _____

Q2.: A sua máquina tem um endereço IPv6?
☑ Sim, tem.
☐ Nem sei bem o que isso significa.

Q3.: Qual o nome da rede IPv4 em que se insere a sua máquina?

☐ 192.168.300.301. ☐ 192.168.1.1.
☑ 10.0.2.0. ☐ 10.0.2.255.
☐ 192.168.0.0. ☐ 310.1.0.0.

Q4.: Como é que se pode especificar a gama de 255 endereços na rede que indicou acima?
☑ Escrevendo o nome da rede seguido de `/24`.
☐ Escrevendo o nome da rede seguido de `/30`.
☐ Escrevendo 127.0.0.1.
☐ Escrevendo o IP da minha máquina seguido de `/30`.

Tarefa 2 *Task 2*

Utilize a ferramenta `nmap` e a informação acumulada na tarefa anterior para obter a lista de endereços de máquinas atualmente ligadas no laboratório (indique o comando que utilizar a seguir) e responda às questões incluídas em baixo.

$ nmap -sn 10.0.2.0/24

Q5.: Que comando / opções utilizou?
☐ `-s` ☐ `-P` ☐ `-sP` ☐ `-sM`

Q6.: De que forma é que o `nmap` identifica as

máquinas ligadas?

- ☑ Enviando pacotes *Transmission Control Protocolo* (TCP) SYN para todas as máquinas e considerando que estão ligadas todas aquelas para que recebe uma resposta.
- ☐ Enviando pacotes TCP SYN para todas as máquinas e considerando que estão ligadas todas aquelas para as quais não recebe uma resposta.
- ☐ Enviando pacotes *Internet Control Message Protocol* (ICMP) do tipo *echo request* para todas as máquinas e considerando que estão ligadas aquelas para que recebe uma resposta.
- ☐ Enviando pacotes ICMP do tipo *echo reply* para todas as máquinas e considerando que estão ligadas aquelas para que recebe uma resposta.

Q7.: Tomou nota dos endereços *Internet Protocol* (IP) das máquinas ligadas à rede?

- ☑ Eh... sim, tomei.
- ☐ Eh... não, não tomei. Era para tomar?

Q8.: Consegue identificar, pelo IP, alguma dessas máquinas imediatamente?

- ☐ Assim de repente, não.
- ☑ Consigo: o *Gateway*.
- ☐ Consigo: a impressora.
- ☐ Consigo: *switches*.
- ☐ Consigo: todos.

2 Identificação do Sistema Operativo

Operating System Identification

Tarefa 3 *Task 3*

A próxima tarefa consiste em **identificar** (ou tentar identificar) **o sistema operativo dos servidores** no laboratório. De modo a reduzir o tráfego que se vai gerar, junte-se com um ou dois colegas para fazer esta tarefa e peça ao Professor para reduzir o número de IPs a testar. Endereços IP a testar:

IP1: _____ . _____ . _____ . _____

IP2: _____ . _____ . _____ . _____

Procure o significado e use uma (ou duas) das seguintes opções para montar o comando necessário, escrevendo-o em baixo:

`-s` `nmap` `-sX` `-O` `-vv`

$ nmap -O 10.0.2.178

Q9.: A que conclusões é que chegou?

A máquina com IP ____ . ____ . ____ . ____ corre o sistema operativo Windows 2000 Server .

A máquina com IP ____ . ____ . ____ . ____ corre o sistema operativo _____ .

Se utilizar o comando para identificação de sistema operativo com a opção `-vv`, vai obter alguma informação adicional acerca do funcionamento do `nmap` para estas situações. **Q10.: Utilizando esta opção, consegue ver a assinatura que foi usada na identificação?**

- ☐ Sim, consigo.
- ☐ Não. Nada.

Considere ainda analisar o *output* gerado pelo comando e opção anterior. Alguns detalhes reportam a facilidade com que se adivinha a forma como os números de sequência TCP e IP são gerados. Note que estes resultados são também usados para determinar o sistema operativo em utilização. **Q11.: Para uma máquina *Windows*, o é que `nmap` tem a dizer sobre isto?**

- ☐ As sequências são previsíveis.
- ☐ As sequências são aleatórias.
- ☑ Algumas são difíceis de prever, outras são incrementais ou fáceis de prever.

Nota: faça, quando possível (i.e., adiante neste laboratório), o mesmo teste para máquinas com sistema operativo Linux ou *Hewlett Packard* (HP) e compare os resultados.

Q12.: Qual é o endereço IP do *Gateway* da rede?

- ☐ Do que?
- ☐ Como é que vejo isso?
- ☐ O endereço é 10 . 0 . 2 . 1 .

Q13.: Já agora, qual é o sistema operativo do *gateway* da rede?

- ☐ É um sistema operativo da família Linux.
- ☐ É um sistema operativo da família Windows.
- ☐ É um sistema operativo da família HP.
- ☐ É um sistema operativo da família MAC OS.

Tarefa 4 *Task 4*

Q14.: Qual dos seguintes identifica a sua própria máquina ou é um endereço IP do *localhost*?

- ☐ 127.1.1.1
- ☐ 127.2.2.1
- ☐ 127.0.0.234
- ☐ 127.0.0.1

Experimente fazer a deteção do sistema operativo para a sua própria máquina. **Q15.: Qual o comando que utilizou?**

$ _____

Q16.: Conseguiu fazer a deteção do sistema operativo que corre na sua máquina?
☐ Que engraçado: não. ☐ Claro que consegui!

Q17.: Qual é o motivo por detrás da resposta anterior?
☐ Este computador não tem perfil de servidor e não tem nenhum serviço a correr!
☐ Este computador não tem perfil de servidor e os serviços que tem a correr não são suficientes para fazer a deteção do sistema operativo.
☐ Este computador tem uma *firewall* muito boa!
☑ Este computador tem perfil de servidor ou serviços suficientes a correr para que a identificação se faça com sucesso.

Q18.: Já experimentou desligar alguns desses serviços (e.g., `$ systemctl stop sshd`) e tentar novamente?
☑ Ainda não experimentei. Mas como sou um aficionado, vou experimentar.
☐ Não... e agora estou com pressa porque tenho uma consulta às 17h00.

Tarefa 5 *Task 5*

Procure a opção que lhe imprime as probabilidades associadas à deteção de um sistema operativo e repita novamente a tarefa anterior. **Q19.: Qual o comando que utilizou?**

$ _____

Caso não tenha sucesso na tarefa anterior, experimente emitir o comando na direção de um servidor Windows.

3 Identificação de Serviços e Respetivas Versões a Correr nos Servidores

Identification of Services and Respective Versions Running on the Servers

Tarefa 6 *Task 6*

Q20.: Qual dos seguintes comandos lhe permitem identificar os serviços (e a sua versão) que estão a correr no sistema operativo *Microsoft Windows Server*?

```
$ nmap -t IPServidor
$ nmap -O IPServidor
$ nmap -sI IPServidor
$ nmap -sV IPServidor   <- este
```

Nota: use o endereço IP do servidor facultado pelo docente no início deste laboratório.

Tarefa 7 *Task 7*

Coloque um servidor *HyperText Transfer Protocol* (HTTP) a correr na sua máquina. Caso não saiba como fazer isso, experimente a seguinte sequência de comandos:

`$ su` (palavra-passe do `root`)

```
$ service httpd start
```

ou

```
$ systemctl start httpd
```

Caso o servidor não esteja instalado, instá-le-o com o seguinte comando:

```
$ dnf install httpd
```

Nota: pode ser preciso desligar a *firewall* com `$ systemctl stop firewalld`[1].

Depois de o colocar a correr, use o `nmap` para identificar a versão do servidor HTTP que acabou de instalar e escreva-a a seguir:

Versão _____.

Tarefa 8 *Task 8*

A próxima tarefa consiste em procurar vulnerabilidades para os serviços que identificou na Internet. Comece a sua procura por `http://www.securityfocus.com/bid`. Note: não quer dizer que chegue a encontrar uma vulnerabilidade para o serviço em questão. A ideia é ficar a conhecer a base de dados acima indicada.

Tarefa 9 *Task 9*

Tome as providências que achar necessárias para responder às questões seguintes.

Q21.: Encontrou alguma impressora de rede durante as suas incursões?
☐ Sim. ☐ Não, mas até já me sinto deslocado.

Q22.: Qual a marca e modelo?

[1] O ideal é adicionar uma regra para deixar estabelecer ligações na porta 80 via

```
$ firewall-cmd --zone=public --add-port=80/tcp
--permanent
```

e reiniciar com `$ firewall-cmd --reload`.

Marca
☐ Brother. ☑ HP. ☐ Cannon. ☐ Epson.
Modelo
☐ SP302. ☐ Stylus. ☑ LaserJet. ☐ EasyJet.

Q23.: Quais as portas disponíveis para este equipamento?

Porta: _____ Serviço: _____

Porta: _____ Serviço: _____

Porta: _____ Serviço: _____

Porta: _____ Serviço: _____

Porta: _____ Serviço: _____

Porta: _____ Serviço: _____

Porta: _____ Serviço: _____

Q24.: Há alguma porta que lhe pareça ser de configuração da impressora?

☑ Sim, a porta _____.
☐ Não.

Q25.: Já tentou aceder via ☐ *browser* ☐ telnet ☐ ssh a essa porta?
☐ Sim, porque sou rápido.
☐ O prof. ainda não me deu tempo para isso.

4 Análise dos Efeitos de um Ataque

Analysis of the Effects of an Attack

Mesmo não descobrindo qualquer vulnerabilidade nos sistemas em questão, é possível efetuar alguns ataques aos sistemas com sucesso (ou talvez não). E.g., se temos servidores HTTP e queremos deixar o serviço indisponível durante algum tempo, podemos sempre tentar um *Denial of Service* (DoS) recorrendo a uma inundação de pedidos SYN. Para esta tarefa, precisamos de um programa que forje pedidos TCP rapidamente e que, possivelmente, falsifique o endereço fonte de onde os pedidos vieram. **Q26.: Qual a motivação principal para forjar o endereço fonte?**
☐ O sucesso do ataque depende do facto do endereço fonte ser forjado.
☐ A ideia é não deixar rasto.
☐ O endereço fonte tem de ser o mesmo da impressora, pelo que tem de ser forjado.
☐ A ideia é não lidar com todas as respostas que o ataque gera.
☐ A ideia é culpar outra pessoa.

Q27.: O que significa SYN?
☐ Significa *Sign Year Network*.
☑ Significa *Syncronization*.
☐ Significa *Start Yes Now*.
☐ Significa *pecado* em português.
☐ Era uma baleia gigante que atormentava o mundo de *Spira* no videojogo *Final Fantasy X*.

Tarefa 10 *Task 10*

Verifique se tem o programa `hping3` instalado na sua distribuição de Linux (faça, e.g., `$ hping3 --help`). Se não tiver o programa instalado, instale-o:

- Em Ubuntu:
  `$ sudo apt-get install hping3`
- Em Fedora:
  `$ su` (seguido da palavra-passe do `root`)
  `$ DNF install hping3`

Tarefa 11 *Task 11*

Tendo a ferramenta `hping3` instalada, aceda ao servidor HTTP que vai atacar usando, por exemplo, o *browser*. Sugestão: pode aceder ao servidor do(a) seu(ua) colega do lado. Procure construir o comando `hping3` que lhe permite atacar a máquina que escolheu, mas com um endereço IP fonte de uma máquina vizinha à sua. Para isso, tenha em conta a seguinte sugestão:

```
$ hping3 --flood -a _____
-_ -p _____ IP_vitima
```

Q28.: Qual a opção/letra que falta a seguir ao - para que o ataque de inundação seja do tipo SYN?
☐ R ☐ S ☐ T ☐ Y ☐ Z

Ao mesmo tempo que faz o ataque, peça a um colega que tente abrir o site do servidor vítima e relate o que observa. Note que este exercício serve o único propósito de demonstrar a facilidade de executar este ataque e os efeitos nefastos que daí possam provir. **Abstenha-se completamente de conduzir este tipo de actividade fora do ambiente laboratorial.**

5 Captura e Observação de Tráfego

Capturing and Observing Traffic

Tarefa 12 *Task 12*

Explore as funcionalidades do programa `tcpdump`. Para o ajudar nesta tarefa, identifique, por exemplo, o que é que faz o comando `tcpdump` com seguinte sequência de opções (caso o `tcpdump` não esteja instalado, proceda à instalação através de um comando semelhante a `$ dnf install tcpdump`):

```
$ sudo tcpdump -i eth0 -A -v -t
```

`-i`

`-A`

`-v`

`-t`

Tarefa 13 *Task 13*

Experimente correr o comando que se segue em simultâneo com o anterior e relate o que vê:

```
$ hping3 -flood -S -p 80 IP_vitima
```

Tarefa 14 *Task 14*

Experimente correr a seguinte combinação de comandos:

```
$ sudo tcpdump -i eth0 -s 1500 -A -v -t |
grep passw
```

enquanto acede ao *site* `http://www.di.ubi.pt/~inacio/lab8.php` e insere as credenciais `lab8` e `palavra-passe-fraca`. **Q29.: O que pode concluir deste exercício?**

- ☐ Que o protocolo HTTP já oferece algumas garantias de segurança.
- ☑ Que o protocolo HTTP não oferece garantias de segurança.
- ☐ Que só conseguimos ver algo porque a palavra-passe era fraca, neste caso.
- ☑ Que as credenciais que inseri viajaram desde o computador que estou a usar, passando pelo *Gateway* e *router* do centro de informática, até que chegou ao servidor destino, sempre em texto-limpo e, ainda por cima, identificados pela palavra `Password`.

Q30.: Como é que o problema anterior se pode resolver em ligações HTTP?

- ☐ Usando palavras-passe maiores e melhores.
- ☑ Ativando o *Transport Layer Security*.
- ☐ Este problema não se pode resolver.
- ☑ Usando outras técnicas de autenticação mais elaboradas.