

Roteiro 2 - Leonardo Malta

1) Descobrir o ip do host no Kali:

- sudo su
- arp-scan -l

Retorna a uma lista de hosts na rede e seus respectivos IPs e Mac address.
Olhando para o Mac Address, a que inicia com 08:00:27 evidencia que é uma máquina virtual.

2) Descobrir qual serviço está rodando na porta 21 (Netcat):

- netcat -z -n -v 172.16.8.18 21

Retornou que está rodando o serviço ftp

3) Descobrir o sistema operacional do Host (Telnet):

- telnet 172.16.8.18 22

Retornou o sistema operacional Debian-8

4) Criação de Escaneamento de Portas com Python:

Script no github: <https://github.com/leonardodma/teckHack.git>

Código baseado em: <https://www.geeksforgeeks.org/port-scanner-using-python/>

5) Listar as vulnerabilidades das portas 21 e 445:

- nmap -sV --script vuln 172.16.8.18 -p21,445

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPD version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2011-2523 BID:48539
| vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command: id
| Results: uid=0(root) gid=0(root)
| References:
| https://www.securityfocus.com/bid/48539
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:1D:FC:A5 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

6) Encontrar um exploit para uma vulnerabilidade nos serviços testados no exercício anterior:

- nmap -sV --script malware 172.16.8.18 -p21,445

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:CVE-2011-2523 BID:48539
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/
|   vsftpd_234_backdoor.rb
|   https://www.securityfocus.com/bid/48539
|_
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:1D:FC:A5 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

7) Encontrar uma CVE classificada como alta para os serviços das portas 3306 e 5432:

- nmap -sV --script vuln 172.16.8.18 -p3306
- nmap -sV --script vuln 172.16.8.18 -p5432

Para a porta 3306, foram encontradas as seguintes cvms classificadas como altas ou críticas:

- **CVE-2009-0226** 8.5: <https://vulners.com/cve/CVE-2009-0226>
- **CVE-2008-0226** 7.5: <https://vulners.com/cve/CVE-2008-0226>

Já para a porta 5432:

- **CVE-2013-1903** 10.0: <https://vulners.com/cve/CVE-2013-1903>
- **CVE-2013-1902** 10.0: <https://vulners.com/cve/CVE-2013-1902>
- **POSTGRESQL:CVE-2013-1900** 8.5: <https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900>
- **CVE-2010-1447** 8.5: <https://vulners.com/cve/CVE-2010-1447>
- **CVE-2010-1447** 8.5: <https://vulners.com/cve/CVE-2010-1447>

8) Realize uma consulta ao nome www.ietf.org, e responda:

a) Qual é o endereço IP associado?

```
leonardodma@ubuntu:~$ nslookup www.ietf.org
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.ietf.org canonical name = www.ietf.org.cdn.cloudflare.net.
Name:   www.ietf.org.cdn.cloudflare.net
Address: 104.16.44.99
Name:   www.ietf.org.cdn.cloudflare.net
Address: 104.16.45.99
Name:   www.ietf.org.cdn.cloudflare.net
Address: 2606:4700::6810:2c63
Name:   www.ietf.org.cdn.cloudflare.net
Address: 2606:4700::6810:2d63
```

b) Quais são seus servidores DNS?

```
leonardodma@ubuntu:~$ host -t ns ietf.org
ietf.org name server ns1.yyz1.afilias-nst.info.
ietf.org name server ns1.sea1.afilias-nst.info.
ietf.org name server ns1.hkg1.afilias-nst.info.
ietf.org name server ns1.ams1.afilias-nst.info.
ietf.org name server ns1.mia1.afilias-nst.info.
ietf.org name server ns0.amsl.com.
```

c) Existe algum servidor de e-mail associado ao domínio ietf.org? Qual o seu nome e IP?

- Utilizando DNS Checker:

<https://dnschecker.org/mx-lookup.php?query=www.ietf.org&dns=cloudflare>

A partir dessa consulta, é possível concluir que o servidor MX é o mail.ietf.org

9) Escolha um site na Internet e responda as seguintes perguntas:

Site escolhido: <https://www.insper.edu.br/>

a) Quais servidores DNS são responsáveis por este domínio? (print a sua consulta)

```
leonardodma@ubuntu:~$ host -t ns insper.edu.br
insper.edu.br name server ns2-07.azure-dns.net.
insper.edu.br name server ns1-07.azure-dns.com.
insper.edu.br name server ns3-07.azure-dns.org.
insper.edu.br name server ns4-07.azure-dns.info.
```

b) Existem outros domínios ou serviços hospedados no mesmo host (IP)? Quais são?

Usando o comando `nslookup www.insper.edu.br`, obtem-se o ip 23.4.192.41. Usando o site <https://hackertarget.com/reverse-ip-lookup/> para encontrar as ocorrências de

hóspedes com esse IP, é encontrado apenas uma ocorrência. Logo, há apenas um domínio hospedado nesse host.

- c) Qual o Servidor WEB e Sistema Operacional que hospedam este site? Quais foram as últimas alterações?


Ao pingar, o ttl retornado é 56 (indicando ser um linux). Usando o comando nmap -O 23.4.192.41, as respostas retornadas foram:

Crestron XPanel control system (90%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%), Linux 4.0 (86%), MikroTik RouterOS 6.36 (86%), Linux 4.4 (85%)

- d) Quais tecnologias (jquery, utilizadas por este site)?

CMS	Automação de Marketing
 WordPress 5.9.3	 HubSpot
Ferramenta Estatística	Banco de Dados
 Google Call Conversion Tracking	 MySQL
 Matomo Analytics	Rede de Publicidade
 LinkedIn Insight Tag	 Criteo
 Hotjar	 Teads
 Google Ads Conversion Tracking	 Microsoft Advertising
 Facebook Pixel	Gestor de Tags
 Microsoft Clarity 0.6.40	 Google Tag Manager
 HubSpot Analytics	Ferramenta de Desenvolvimento
 Google Analytics	 styled-components 4.3.2

Blog

 [WordPress](#) 5.9.3

Framework JavaScript

 [React](#)

 [styled-components](#) 4.3.2


Security


 [Akamai Web Application Protector](#)

Script de Fonte

 [Twitter Emoji \(Twemoji\)](#)


Diversos

 [Open Graph](#)

 [parcel](#)

 [Babel](#)


Servidor Web


 [Apache](#)

Linguagem de Programação


 [PHP](#)

CDN

 [Akamai](#)

 [Google Hosted Libraries](#)


Chat Direto


 [WhatsApp Business Chat](#)

SEO


 [Yoast SEO](#) 8.0

Biblioteca JavaScript

 [Preact](#)

 [FancyBox](#) 3.3.5

 [core-js](#) 2.6.9

 [OWL Carousel](#)

 [jQuery Migrate](#) 3.3.2

 [jQuery](#) 2.1.3

UI Frameworks

 [Bootstrap](#) 3.3.7

Retargeting

 [Criteo](#)

WordPress plugins

 [Yoast SEO](#) 8.0

 [GTranslate](#)

Translation

 [GTranslate](#)

- e) Existe algum WAF protegendo este site? (Print a saída do comando)
Não foi detectado nenhum WAF:

```
leonardodma@ubuntu:~$ wafw00f -a -v www.insper.edu.br

{ W00F! }

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.insper.edu.br
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
```

f) O Domínio possui um servidor de e-mail configurado? Qual (is) Ip (s)?

- Utilizando o DNS Checker:

<https://dnschecker.org/mx-lookup.php?query=www.insper.edu.br&dns=google>

É possível concluir que o servidor de emails é o esa2.hc2847-56.iphmx.com, com o IP 216.71.140.122

10) Utilizando sua ferramenta (port scan) descubra quais portas TCP e UDP estão abertas no alvo, bem como os serviços que estão associados nestes. Pesquise e anote em seu diário de bordo as vulnerabilidades comuns conhecidas (CVE) do processo que está gerenciando a porta 21.

```
Leonardodma@ubuntu:~/Documentos/teckHack/roteiro_2$ python3 portScanner.py
IP a ser escaneado: 192.168.15.15  → portScanner.py M X
Porta 1: 1
Porta 2 (A maior existente é a 65535): 65535
Começando Scan em 192.168.15.15, da porta 1 até a porta 65535:

A Porta 21 está aberta:      3 ip = input("IP a ser escaneado: ")
Rodando o Serviço TCP: ftp    4 port1 = int(input("Porta 1: "))
Rodando o Serviço UDP: fsp    5 port2 = int(input("Porta 2 (A maior
=====do Scan em (ip), da
A Porta 22 está aberta:      7
Rodando o Serviço TCP: ssh    8 for port in range(port1, port2):
===== socket.socket(socket.AF_INET
A Porta 23 está aberta:      10 if s.connect_ex((ip, port)) == 0:
Rodando o Serviço TCP: telnet 10 print(f"A Porta (port) está
=====
A Porta 25 está aberta:      12 service_tcp = socket.get
Rodando o Serviço TCP: smtp   13 print(f"Rodando o Servi
===== except:
A Porta 53 está aberta:      15 pass
Rodando o Serviço TCP: domain 16
Rodando o Serviço UDP: domain 17
=====
A Porta 111 está aberta:     19 service_udp = socket.get
Rodando o Serviço TCP: sunrpc 20 print(f"Rodando o Servi
Rodando o Serviço UDP: sunrpc 21 except:
=====
A Porta 139 está aberta:     23
Rodando o Serviço TCP: netbios-ssn 24 print("=====
=====
A Porta 445 está aberta:     26 s.close()
Rodando o Serviço TCP: microsoft-ds 26
=====
A Porta 512 está aberta:
Rodando o Serviço TCP: exec
Rodando o Serviço UDP: biff
```

```
A Porta 513 está aberta:
Rodando o Serviço TCP: login  → portScanner.py M X
Rodando o Serviço UDP: who
=====
A Porta 514 está aberta:     1 import socket
Rodando o Serviço TCP: shell  2
Rodando o Serviço UDP: syslog 3 ip = input("IP a ser escaneado: ")
===== port1 = int(input("Porta 1: "))
A Porta 1099 está aberta:     5 port2 = int(input("Porta 2 (A maior
===== print(f"Começando Scan em (ip), da
=====
A Porta 1524 está aberta:     8 for port in range(port1, port2):
Rodando o Serviço TCP: ingreslock 9 s = socket.socket(socket.AF_INET
===== s.connect_ex((ip, port)) == 0
A Porta 2049 está aberta:     11 print(f"A Porta (port) está
Rodando o Serviço TCP: nfs    12 try:
Rodando o Serviço UDP: nfs    13 service_tcp = socket.get
===== print(f"Rodando o Servi
A Porta 2121 está aberta:     15 except:
Rodando o Serviço TCP: iprop  16 pass
=====
A Porta 3306 está aberta:     18 try:
Rodando o Serviço TCP: mysql  18 service_udp = socket.get
===== print(f"Rodando o Servi
A Porta 3632 está aberta:     20 except:
Rodando o Serviço TCP: distcc 21
=====
A Porta 5432 está aberta:     23 print("=====
Rodando o Serviço TCP: postgresql 24
=====
A Porta 5900 está aberta:     26 s.close()
=====
A Porta 6000 está aberta:
Rodando o Serviço TCP: x11
=====
A Porta 6667 está aberta:
Rodando o Serviço TCP: ircd
```

```

A Porta 6697 está aberta:
Rodando o Serviço TCP: ircs-u
=====
A Porta 8009 está aberta:
=====
A Porta 8180 está aberta:
=====
A Porta 8787 está aberta:
=====
A Porta 37890 está aberta:
=====
A Porta 39710 está aberta:
=====
A Porta 46718 está aberta:
=====
A Porta 49748 está aberta:
=====

```

As vulnerabilidades mais comuns na porta 21 são:

- [CVE-2019-19296](#): O servidor de vídeo SiVMS/SiNVR permite um acesso de modo que o Hacker consiga um acesso autenticado para fazer downloads de qualquer arquivo.
- [CVE-2017-6872](#): permite que o atacante que tenha acesso à porta 21, e consiga alterar dados históricos no dispositivo.
- [CVE-2020-10288](#): Ao tentar obter acesso do serviço ftp exposto pelo IRC5, qualquer campo não vazio é aceito como login e senha.
- CVE-2018-10070: vulnerabilidade no MikroTik Version 6.41.4, permite que um atacante esgote toda a CPU e RAM disponível enviando uma solicitação de FTP criada na porta 21 que começa com muitos caracteres '\0'.

Referências:

- <https://makandracards.com/makandra/41662-how-to-find-out-what-is-running-on-a-port-on-a-remote-machine>
- <https://geekflare.com/nmap-vulnerability-scan/>
- <https://www.geeksforgeeks.org/port-scanner-using-python/>
- https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=port+21&queryType=phrase&search_type=all&isCpeNameSearch=false
- Slides da matéria