

Diário de Bordo - Roteiro 2

Abel Cavalcante

1.1.a. Descubra qual ip do seu alvo.

Usando o comando *ifconfig* dentro do sistema metasploitable, é possível ver que o IP designado para a máquina foi *192.168.56.101*.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:86:07:ad
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe86:7ad/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Fig 1. - IP usando ifconfig

Usando o Kali linux, é possível confirmar esse endereço pelo navegador:

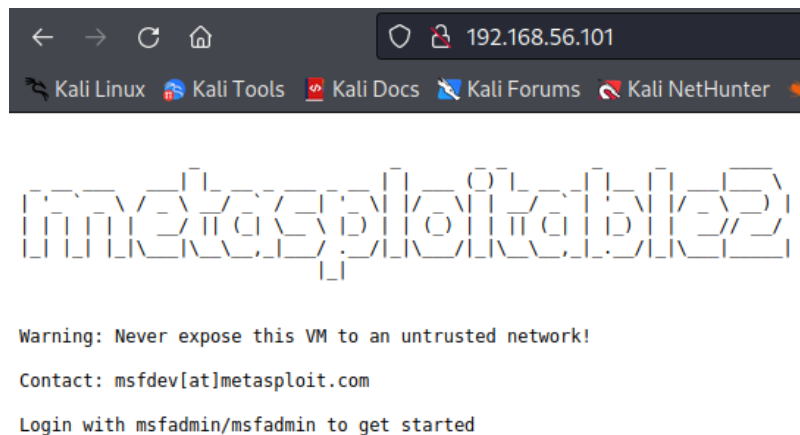


Fig 2. - Acesso pelo Kali

1.1.b. Reconhecendo serviços e portas abertas do alvo.

Para reconhecer a porta 21, o processo e a versão foi usado o seguinte comando:

```
(root@kali)-[/home/kali]
# nc 192.168.56.101 21
220 (vsFTPd 2.3.4)
```

Fig 3. - Netcat usado para ler o serviço da porta 21

1.1.c. Fingerprint:

Na coleta de informações, foi usado o comando `nmap -v -A 192.168.56.101`, onde:

- -v: Aumenta a verbosidade da saída;
- -A: Habilita identificação de OS, versão, escaneamento de saída e rotas de tráfego.

Nesse comando, é possível ver as portas abertas:

```
Scanning 192.168.56.101 [1000 ports]
Discovered open port 139/tcp on 192.168.56.101
Discovered open port 22/tcp on 192.168.56.101
Discovered open port 80/tcp on 192.168.56.101
Discovered open port 3306/tcp on 192.168.56.101
Discovered open port 21/tcp on 192.168.56.101
Discovered open port 53/tcp on 192.168.56.101
Discovered open port 111/tcp on 192.168.56.101
Discovered open port 25/tcp on 192.168.56.101
Discovered open port 23/tcp on 192.168.56.101
Discovered open port 445/tcp on 192.168.56.101
```

Fig 4. - Exemplo de algumas portas abertas no host

É possível ver também o serviço que cada porta executa, bem como a rota de tráfego e informações sobre o OS:

```
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec      netkit-rsh rexecd
513/tcp open  login
514/tcp open  shell     Netkit rshd
1099/tcp open  java-rmi  GNU Classpath grmiregistry
1524/tcp open  bindshell Metasploitable root shell
2049/tcp open  nfs       2-4 (RPC #100003)
2121/tcp open  ftp       ProFTPD 1.3.1
3306/tcp open  mysql     MySQL 5.0.51a-3ubuntu5
```

Fig 5. - Exemplo de alguns serviços rodando em cada porta

```
Aggressive OS guesses: QEMU user mode network gateway (95%), Bay Networks Bay
88%), GNU Hurd 0.3 (88%), Allied Telesyn AT-9006SX/SC switch (88%), Linux 2.6
Virtualbox (87%), Bay Networks BayStack 450 switch (software version 4.2.0.1
No exact OS matches for host (test conditions non-ideal).
```

Fig 6. - Estimativa de OS feita pelo Nmap

```
TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.51 ms  10.0.2.2
2   1.01 ms  192.168.56.101
```

Fig 7. - Roteamento da máquina

1.1.d. Código em Python:

Link do GitHub: https://github.com/FidyBack/port_searcher

Referências para o código:

[[Basic Port Scanner](#)][[Port Scanner in Python](#)][[How to Write a Port Scanner](#)][[Port Scanner in Python](#)][[Use Python to Translate Ports](#)][[Text Align - StackOverflow](#)][[Socket address family - IBM](#)][[TCP/IP and Sockets](#)][[Socket Types - Oracle](#)]

1.1.e. Listar as vulnerabilidades das portas 21 e 445:

Na porta 21, foram encontradas as seguintes vulnerabilidades:

- ftp-vsftpd-backdoor

```
(root@kali)-[/home/kali]
# nmap -sV -p 21 --script vuln 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 05:30 EST
Nmap scan report for 192.168.56.101
Host is up (0.00051s latency).

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://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_  https://www.securityfocus.com/bid/48539
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.45 seconds
```

Fig 8. - Vulnerabilidades apontadas pelo nmap na porta 21

Porta 445, o comando não apresentou nenhuma vulnerabilidade, apesar de possuir a porta aberta.

```
(root@kali)-[/home/kali]
# nmap -sV -p 445 --script vuln 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 05:43 EST
Nmap scan report for 192.168.56.101
Host is up (0.00028s latency).

PORT      STATE SERVICE VERSION
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.38 seconds
```

Fig 9. - Vulnerabilidades apontadas pelo nmap na porta 445

1.1.f. Encontrar um exploit para uma vulnerabilidade nos serviços testados no exercício anterior.

Como a versão usada na porta 21 é a *vsftpd - 2.3.4*, é possível usar o comando `searchsploit` para encontrar exploits dessa versão:

```
(root@kali)-[/home/kali]
# searchsploit vsftpd | grep 2.3.4
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
```

Fig 10. - Exploits possíveis na porta 21, usando a versão 2.3.4 do vsftpd

Já porta 445, é possível usar o seguinte comando para [encontrar a versão exata](#):

```
(root@kali)-[/home/kali]
# nmap -sV -p 445 -sC 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 06:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00050s latency).

PORT      STATE SERVICE      VERSION
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2022-03-06T06:02:35-05:00
|_clock-skew: mean: 2h29m58s, deviation: 3h32m08s, median: -2s
```

Fig 11. - Método usado para descobrir a versão do Samba utilizado

Sabendo agora que a versão usada é a *Samba - 3.0.20*, é possível ir atrás dos exploits usando o `searchsploit`:

```
(root@kali)-[/home/kali]
# searchsploit Samba | grep 3.0.20
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow | linux/remote/7701.txt
```

Fig 12. - Exploits possíveis na porta 445, usando a versão 3.0.20 do Samba

1.1.g. Encontrar uma CVE classificada como alta para os serviços das portas 3306 e 5432.

Usando o script do nmap na porta 3306, a CVE com o maior score de acordo com o CVSS foi a CVE-2009-2446.

```
(root@kali)-[/home/kali]
# nmap -sV -p 3306 --script vuln 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 07:08 EST
Nmap scan report for 192.168.56.101
Host is up (0.00062s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| vulners:
|   cpe:/a:mysql:mysql:5.0.51a-3ubuntu5:
|   SSV:19118      8.5    https://vulners.com/seebug/SSV:19118    *EXPLOIT*
|   CVE-2009-2446  8.5    https://vulners.com/cve/CVE-2009-2446
```

Fig 13. - CVE com maior score dentro da porta 3306

Já dentro da porta 5432, foram encontradas 2 CVEs com o score máximo: a CVE-2013-1902 e CVE-2013-1903:

```
(root@kali)-[/home/kali]
# nmap -sV -p 5432 --script vuln 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 07:13 EST
Nmap scan report for 192.168.56.101
Host is up (0.0011s latency).

PORT      STATE SERVICE      VERSION
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| vulners:
|   cpe:/a:postgresql:postgresql:8.3:
|   SSV:60718      10.0    https://vulners.com/seebug/SSV:60718    *EXPLOIT*
|   CVE-2013-1903  10.0    https://vulners.com/cve/CVE-2013-1903
|   CVE-2013-1902  10.0    https://vulners.com/cve/CVE-2013-1902
```

Fig 14. - CVEs com maior score dentro da porta 5432

1.1.h. Realize uma consulta ao nome www.ietf.org, e responda:

a. Qual é o endereço IP associado?

Ip: 104.16.45.99 (Possui um IP extra: 104.16.44.99);

b. Quais são seus servidores DNS?

Servidores DNS: Cloudflare

```
(root@kali)-[/home/kali]
# nikto -h www.ietf.org
- Nikto v2.1.6

+ Target IP:          104.16.45.99
+ Target Hostname:    www.ietf.org
+ Target Port:        80
+ Message:            Multiple IP addresses found: 104.16.45.99, 104.16.44.99
+ Start Time:         2022-03-06 07:28:56 (GMT-5)

+ Server: cloudflare
```

Fig 15. - Comando e resposta dada pelo nikto para aquisição do IP e DNS

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

Esse domínio aparenta ter um servidor de email:

```
(root@kali)-[/home/kali]
# host www.ietf.org
www.ietf.org is an alias for www.ietf.org.cdn.cloudflare.net.
www.ietf.org.cdn.cloudflare.net has address 104.16.45.99
www.ietf.org.cdn.cloudflare.net has address 104.16.44.99
```

Fig 16. - Comando e resposta com nome e IP do servidor de email

Pelo nome, pode ser um [email externo/filtro de spam](#).

1.1.i. Escolha um site na Internet e responda às seguintes perguntas:

Site escolhido: michaelreeves.us;

Servidores DNS: ns3.digitalocean.com; ns2.digitalocean.com; ns1.digitalocean.com.

Domínio encontrado	OK	O domínio michaelreeves.us foi encontrado na consulta dos Root-Servers Resposta obtida do servidor: Y.CC.TLD.US
Servidores DNS Reportados	INFO	Os seguintes servidores DNS foram reportados como responsáveis pelo seu domínio: ns3.digitalocean.com. [198.41.222.173] [SEM GLUE] ns2.digitalocean.com. [173.245.59.41] [SEM GLUE] ns1.digitalocean.com. [173.245.58.51] [SEM GLUE]

Fig 17. - Servidores DNS tirados do site <https://ipok.com.br/>

Domínios no mesmo IP: Nenhum

Known Websites on IP - 138.68.54.188						
No	Web Site	Website IP Address	Web Hosting Company / IP Owner	Web Hosting / Server IP Location	Record Update Time	World Site Popular Rating
1	michaelreeves.us	138.68.54.188	DigitalOcean, LLC	USA	04 Mar 2022, 00:10	# 7,350,959

Total: 1 record

Fig 18. - Domínios DNS tirados do myip.ms

Servidor WEB: nginx/1.10.3

```
(kali@kali)-[~]
$ nikto -h michaelreeves.us
- Nikto v2.1.6

+ Target IP: 138.68.54.188
+ Target Hostname: michaelreeves.us
+ Target Port: 80
+ Start Time: 2022-03-07 22:07:21 (GMT-5)

+ Server: nginx/1.10.3 (Ubuntu)
```

Fig 19. - Servidor WEB do alvo

SO: Linux, mas especificamente, Ubuntu (Usando QEMU ou Virtualbox)

```
(root@kali)-[/home/kali]
# nmap -A michaelreeves.us
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-07 23:00 EST
Nmap scan report for michaelreeves.us (138.68.54.188)
Host is up (0.066s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 9d:65:f1:64:9e:65:17:4d:e0:67:9d:7e:62:dc:65:18 (RSA)
|   256 59:11:7f:a7:e8:13:67:a0:9b:7a:be:70:60:49:38:70 (ECDSA)
|_  256 ad:1f:34:03:05:4b:12:64:5f:85:f1:e8:bd:24:90:93 (ED25519)
80/tcp    open  http      nginx 1.10.3 (Ubuntu)
|_ http-title: Did not follow redirect to https://michaelreeves.us/
|_ http-server-header: nginx/1.10.3 (Ubuntu)
443/tcp   open  ssl/http  nginx 1.10.3 (Ubuntu)
|_ http-title: 400 The plain HTTP request was sent to HTTPS port
|_ tls-nextprotoneg:
|   h2
|_ http/1.1
|_ ssl-cert: Subject: commonName=michaelreeves.us
|_ Subject Alternative Name: DNS:michaelreeves.us, DNS:www.michaelreeves.us
|_ Not valid before: 2020-04-24T11:51:47
|_ Not valid after:  2020-07-23T11:51:47
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|   h2
|_ http/1.1
|_ http-server-header: nginx/1.10.3 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch|printer
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (94%), Bay Networks embedded (87%), Dell embedded (87%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450 cpe:/h:dell:1600n
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (94%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (87%), Dell 1600n printer (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Fig 20. - S.O. do alvo

Tecnologias:










TECHNOLOGIES	MORE INFO	Export
Analytics	CDN	
 Google Analytics	 Google Hosted Libraries	
Font scripts	JavaScript libraries	
 Google Font API	 jQuery 1.12.4	
 Font Awesome	Reverse proxies	
Web servers	 Nginx 1.10.3	
 Nginx 1.10.3	UI frameworks	
Operating systems	 Bootstrap 3.3.7	
 Ubuntu		

Fig 21. - Tecnologias do alvo

WAF: Nenhum

```
(kali㉿kali)-[~]  
$ wafw00f michaelreeves.us
```

Home

Woof!

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

```
[*] Checking https://michaelreeves.us  
[+] Generic Detection results:  
[-] No WAF detected by the generic detection  
[~] Number of requests: 7
```

Fig 22. - WAF inexistente

Domínio do servidor de email: Nenhum

```
(kali㉿kali)-[~]  
$ host michaelreeves.us  
michaelreeves.us has address 138.68.54.188
```

Fig 23. - Servidor de email inexistente

1.1.j. Portas do alvo utilizando o programa feito

```
-----
Procurando por portas abertas
Host: michaelreeves.us
Ip: 138.68.54.188
-----
PORTA  ESTADO  SERVIÇO
22      open    ssh
80      open    http
443     open    https
-----
Completo em 264.6 segundos
```

Fig 24. - Scan das portas com o programa feito em Python