MENU

SECURISM

All about Information Security

OSCP NOTES – INFORMATION GATHERING

DNS

> *nslookup <ip> <Name server>*

DNS ENUMERATION

Name Server : host -t ns <hostname>

Mail Exchange : host -t mx <hostname>

REVERSE DNS ENUMERATION

> *host <ip address>*

DNS ZONE TRANSFER FILE

> *host -l <domain name> <name server>*
>
> *dig @<dns server> <domain> axfr*

DNS ENUMERATION TOOLS

dns-recon

dns-enum

TYPES OF INFORMATION RECORDS

SOA Records – Indicates the server that has authority for the domain.

MX Records – List of a host's or domain's mail exchanger server(s).

NS Records – List of a host's or domain's name server(s).

A Records – An address record that allows a computer name to be translated to an IP address. Each computer has to have this record for its IP address to be located via DNS.

PTR Records – Lists a host's domain name, host identified by its IP address.

SRV Records – Service location record.

HINFO Records – Host information record with CPU type and operating system.

TXT Records – Generic text record.

CNAME – A host's canonical name allows additional names/ aliases to be used to locate a computer.

RP – Responsible person for the domain.

FTP

> *nmap -sV -Pn -vv -p %s –script=ftp-anon,ftp-bounce,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221*

FREEBSD USING OPIE ONE TIME PASSWORD SYSTEM

> *nmap -sV –script=ftp-libopie <target> [DOS]*

DETECTION OF FTP BACKDOOR

```
nmap —script ftp-proftpd-backdoor -p 21 -—script-args exploit.cmd=<>
nmap —script ftp-vsftpd-backdoor -p 21 -—script-args exploit.cmd=<>
```

PROFTPD SERVER, VERSION BETWEEN 1.3.2RC3 AND 1.3.3B

```
nmap —script ftp-vuln-cve2010-4221 -p 21
```

ENUMERATION OF USERS

SOLARIS IN.FTPD

```
ftp-user-enum.pl -U users.txt -t <ip address>
```

SOLARIS IN.FTPGNU INETUTILS FTPD

```
ftp-user-enum.pl -M iu -U users.txt -t <ip address>
```

User enumeration is also possible in following FTP servers as well
BlackMoon FTP Server http://xforce.iss.net/xforce/xfdb/12046
ArGoSoft FTP Server http://xforce.iss.net/xforce/xfdb/18721
MegaBrowser FTP Server http://www.securityfocus.com/archive/1/323813

HTTP

APACHE

```
nmap –script=http-apache-negotiation –script-args http-apache-negotiation.root=/root/ <target>
```

FRONTPAGE ANONYMOUS LOGIN

```
nmap <target> -p 80 –script=http-frontpage-login
```

HTTP PUT METHOD

```
nmap -p 80 <ip> –script http-put –script-args http-put.url=’/uploads_directory/rootme.php’,http-put.file=’/home/nikhil/temp/abcd.htm’
```

IIS SHORT NAME BRUTEFORCE

```
nmap -p80 –script http-iis-short-name-brute 10.xx.xx.xx
```

WORDPRESS SCAN

```
sudo wpscan –url 10.xx.xx.251/wp/ –enumerate –threads 10 –follow-redirection –wp-content-dir /wp/wp-content/
```

NIKTO SCAN

```
nikto -port 80 -host 10.xx.xx.251 -root /wp
```

DIRBUSTER

Use GUI

SHELLSHOCK

```
nmap -sV -p- –script http-shellshock –script-args uri=/cgi-bin/bin,cmd=ls <target>
```

COLDFUSION

http://www.pwnag3.com/2013/04/coldfusion-for-pentesters-part-2.html
https://www.exploit-db.com/docs/17845.pdf
Good resource : http://www.slideshare.net/chrisgates/coldfusion-for-penetration-testers

MSSQL

http://travisaltman.com/pen-test-and-hack-microsoft-sql-server-mssql/

Run nmap on TCP 1433 and UDP 1444

CLIENT

> *sqsh -U sa -S 10.xx.xx.31*

MYSQL

VULNERABILITY

> *nmap -p3306 –script mysql-vuln-cve2012-2122 –script-args mysql-vuln-cve2012-2122.user=root,mysql-vuln-cve2012-2122.pass=” <target>*

USERNAME ENUMERATION

```
nmap –script=mysql-enum –script-args userdb=<username lists>
```

MYSQL CLIENT

```
mysql -h 10.xx.xx.223 -P 3306

mysql -u <user> -p <password>
```

```
ERROR 1130 (HY000): Host ’10.xx.xx.54' is not allowed to connect to this MySQL server
```

Reason: http://stackoverflow.com/questions/19101243/error-1130-hy000-host-is-not-allowed-to-connect-to-this-mysql-server

NTP

> *nmap -sU -p 123 –script ntp-info <target>*

https://www.securepla.net/using-ntp-to-enumerate-client-ips/
http://www.vulnerabilityassessment.co.uk/ntp.htm

RDP

RDP ENUMERATION

Check exact OS

```
rdesktop <IP>
```

Check for MS12-020

```
sudo nmap -sV –script rdp-vuln-ms12-020 -p 3389 10.xx.xx.230
```

Only DOS exploits available.

BRUTEFORCE RDP

```
ncrack -vv –user administrator -P /usr/share/wordlists/nikhil_passwords_OSCP –connection-limit 1 rdp://10.xx.xx.230
```

SMB

WHEN LOGGING IN VIA SMB

Local account : <username>
Domain account : thinc.local\<username>

SMB MAP

https://github.com/ShawnDEvans/smbmap

Can be used to pass hashes also

```
python smbmap.py -u jsmith -p 'aad3b435b51404eeaad3b435b51404ee:da76f2c4c96028b7a6111aef4a50a94d' -H 172.16.0.20
```

SMB NTLM AUTHENTICATION LACK OF ENTROPY VULNERABILITY – CVE-2010-0231

http://www.ampliasecurity.com/advisories/windows-smb-ntlm-authentication-weak-nonce-vulnerability.html

SMB ENUMERATION

```
nmap -p139,445 <ip address>
nmap -p139,445 –script smb-enum-users <ip address>
nmap -p139,445 –script smb-enum-users –script-args=unsafe=1 <ip address>
```

```
nmap -p U:137,T:139,445 -sU -sS –script=smb-os-discovery 10.xx.xx.0/24
```

```
nbtscan <ip address or network>
enum4linux -a <host ip>
enum4linux -a -u <username> -p <password> <host ip>
```

SMB NSE SCRIPTS

```
nmap -p 445 <target> –script=smb-vuln-ms10-054 –script-args unsafe, smb-vuln-ms10-054.share=<>, smbpassword=<>, smbusername=<>
nmap –script smb-vuln-ms08-067.nse -p445 <host>
nmap –script smb-vuln-ms07-029.nse -p445 <host> (only for DNS Servers)
nmap –script smb-vuln-cve2009-3103.nse -p445 <host>
```

Metasploit module : **ms09_050_smb2_negotiate_func_index**

Targets : Windows Vista SP1/SP2 and Server 2008 (x86)

SMB NULL SESSION

```
rpcclient -U “” <ip address>
```

then, blank password

```
rpcclient>srvinfo
rpcclient>enumdomusers
rpcclient>getdompwinfo
```

SMTP

http://blog.cobaltstrike.com/2013/10/03/email-delivery-what-pen-testers-should-know/

SMTP ENUMERATION

Connect to port 25 using nc and use
VRFY <username>
for user existence

HELO – This is the command that the client sends to the server to initiate a conversation. Generally, the IP address or domain name must accompany this command, such as HELO 192.168.101 or HELO client.microsoft.com.
EHLO – This command is the same as HELO, but communicates to the server that the client wants to use Extended SMTP. If the server does not offer ESMTP, it will still recognize this command and reply appropriately.
STARTTLS – Normally, SMTP servers communicate in plaintext. To improve security, the connection between SMTP servers can be encrypted by TLS (Transport Layer Security). This command starts the TLS session.
RCPT – Specifies the email address of the recipient.
DATA – Starts the transfer of the message contents.
RSET – Used to abort the current email transaction.
MAIL – Specifies the email address of the sender.

QUIT – Closes the connection.

HELP – Asks for the help screen.

AUTH – Used to authenticate the client to the server.

VRFY – Asks the server to verify is the email user's mailbox exists.

SNMP

SNMP ENUMERATION

> *nmap -sU -p161 <ip address>*
>
> *onesixtyone -c <community> -i <ip address>*

Gives error when community string is greater than 16chars in dictionary file, but can accept in command line

snmpwalk

snmpenum

snmpcheck

SSH

OPENSSH USERNAME ENUMERATION

> *./ssh_time_attack.py -H 10.xx.xx.125 -p 22 -L /usr/share/wordlists/nikhil_usernames_OSCP -d 20*

https://www.devconsole.info/?p=341

OpenSSH 5.9p1

OpenSSH 5.8p1

OpenSSH 6.0p1

OpenSSH 6.2p2

OpenSSH 5.5p1

OpenSSH 5.3

OpenSSH 5.3p1

VNC

```
medusa -u jd -P /usr/share/wordlists/nikhil_passwords_OSCP -t 5 -h 10.xx.xx.227 -e ns -F -M vnc
```

SHARE THIS:

Twitter Facebook

★ Like

Be the first to like this.

LEAVE A REPLY

Enter your comment here...

Search …

PAGES

- Contact
- OSCP Notes – Buffer Overflow
- OSCP Notes – Exploitation
- OSCP Notes – File Transfers
- OSCP Notes – Information Gathering
- OSCP Notes – Meterpreter
- OSCP Notes – Password Attacks
- OSCP Notes – Port Forwarding
- OSCP Notes – Port Scanning
- OSCP Notes – Privilege Escalation (Linux)
- OSCP Notes – Privilege Escalation (Windows)
- OSCP Notes – Shells