Ethical Hacking: Enumeration - Preconfiguration

with Malcolm Shore

Chapter 2: Profiling a Windows host

Do the following on the Windows 10 system

Start Remote Procedure Call (RPC) service

Start RPC Locator service

Start RPC Endpoint Mapper service

Start Remote Registry service

Adjust registry keys (Run>RegEdit)

HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

- Right-click and select Permissions
- Add, select object type user, and add in IEUser and Check Names
- Set permissions and then Apply

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

- Right click and select Permissions
- Add, select object type user, and add in IEUser and Check Names
- Set permissions and then Apply

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

- Add a new DWORD, LocalAccountTokenFilterPolicy
- Set to value 1

Run Secpol.msc

- disable Accounts: Limit local....

Go to https://technet.microsoft.com/en-us/sysinternals/pstools.aspx and install the PsTools suite

Chapter 3: Enumerating SMB from Linux: Episode 1

Load ShareEnum into Kali

```
wget github.com/CroweCybersecurity/shareenum/releases/download/2.0/ shareenum_2.0_amd64.deb
dpkg -i shareenum_2.0_amd64.deb [enter]
```

Chapter 3: Enumerating SMB from Windows: Episode 1

Install the following tools on the Windows 7 system

https://sourceforge.net/projects/netbiosscan/

https://sourceforge.net/projects/nbtenum/

Install the following tools on the Windows 10 system

www.mitec.cz/netscan.html

Chapter 3: Enumerating SMB from Windows: Episode 2

Install the following tools on the Windows 7 system

https://technet.microsoft.com/en-us/sysinternals/shareenum.aspx

https://www.softperfect.com/products/networkscanner/

Chapter 3: SNMP enumeration

Install snmpenum on Kali

```
cd /usr/share
mkdir snmpenum
cd snmpenum
wget http://dl.packetstormsecurity.net/UNIX/scanners/snmpenum.zip
unzip snmpenum
```

Edit the snmpd defaults on Metasploitable

```
sudo nano /etc/default/snmpd
```

change SNMPDOPTS line address from 127.0.0.1 to 0.0.0.0

Chapter 3: Enumerating with RPC

Install WinFingerprint on the Windows 7 system

http://qpdownload.com/winfingerprint-062zip/

Chapter 3: Using WMI to enumerate Windows

Set up Windows for WMI: Set network to private (right click in network sharing) start RPC Locator, close Firewall, and run winrm quickconfig

Download and extract the WMIE tool from the website

https://wmie.codeplex.com/

Chapter 3: Enumeration using Finger

Install the Finger daemon on Ubuntu

```
sudo apt-get install inetutils-inetd fingerd
/etc/init.d/inetutils-inetd start
sudo ufw allow 79
```

Chapter 4: Tracing Internet routes

Install on the Windows 7 system

https://sourceforge.net/projects/openvisualtrace/?source=typ_redirect

Chapter 4: Enumerating LDAP

Install zmap on Kali

```
apt-get install zmap
```

Chapter 5: Introducing SuperScan

Install SuperScan on the Windows 7 system

http://www.mcafee.com/us/downloads/free=tools/superscan.aspx

Chapter 5: Running NetScan Tools Pro

Install NetScan Tools Pro on the Windows 7 system

http://www.netscantools.com/download.html

Chapter 5: Enumerating LDAP

Update to current level

```
sudo apt-get update
sudo apt-get upgrade
```

If you encounter problems with "Failed to Fetch Files" on apt-get update/upgrade, try adding a new file /etc/resolvconf/resolv.conf.d/tail with two lines

```
nameserver 8.8.8.8
nameserver 4.4.4.4
```

Installing an LDAP service

Refer to https://www.unixmen.com/install-openldap-in-ubuntu-15-10-and-debian-8/

```
sudo apt-get install slapd ldap-utils
```

{complete using your own admin account}

```
sudo nano /etc/ldap/ldap.conf
```

[replace 'BASE' and ' URI' values with your domain name and IP Address]

```
eg:  BASE   c=malcolmshore, dc=com
     URI    ldap://10.0.2.9 ldap://10.0.2.9:666  (using the IP address of Ubuntu host)
```

```
sudo dpkg-reconfigure slapd
```

{complete the configuration using your own entries, repeat the admin account entered above}

[allow LDAP v2]

```
sudo apt-get install phpldapadmin
sudo ln -s /usr/share/phpldapadmin/ /var/www/html/phpldapadmin
sudo nano /etc/phpldapadmin/config.php
[change the following lines as shown]
  $servers->setValue(‘server’,’name’,’MS-LDAP’); {use any name you want}
  $servers->setValue(‘server’,’host’,’10.0.2.9’); {use your Ubuntu IP address}
  $servers->setValue(‘server’,’base’,array(‘dc=malcolmshore,dc=com’)); {use your dc}
....
  $servers->setValue(‘login’,’bind_id’,’cn=admin,dc=malcolmshore,dc=com’); {use your dc}

sudo systemctl restart apache2
sudo ufw allow 80
sudo ufw allow 389
```

Then on a workstation on the network, connect to http://10.0.2.9/phpldapadmin

[login using admin password]

[set up your company records

Install JXplorer on Windows 7

http://www.jxplorer.org/