



**Network Enumeration
exercises
Ethical Hacking lab exercise.**

Note : - The location of the tools folder in the University labs is \\hannah\Tools\Pentest

Note that Information contained in this document is for educational purposes.

Contents

1	Introduction	1
1.1	What is enumeration?	1
1.2	Reminder of the virtual network	2
1.3	Run the servers on the virtual network	3
1.4	DNS Enumeration.....	3
1.5	Analysing the DNS from Windows	4
1.6	Reverse DNS.....	5
1.7	Analysing the DNS from Kali Linux	6
2	Network enumeration using Kali Linux	7
2.1	SMB Enumeration using NBTSCAN	7
2.2	Enumerating shares using SMBMAP	8
2.3	SMB enumeration using RPCCLIENT	9
2.4	SMB Enumeration using POLENUM (Policy Enumerator)	10
2.5	SMB Enumeration using ENUM4LINUX	11
2.6	SMB Enumeration using CRACKMAPEXEC	11
3	Other enumeration techniques	12
3.1	SNMP Enumeration from Kali linux.....	12
3.2	SMTP Enumeration from Kali linux	13
4	Enumeration using Windows.....	14
4.1	Nbtenum3.3	14
4.2	NetBIOS Enumeration using nbtstat	14
4.3	SID2USER/USER2SID	15
	Research exercises	17
4.4	Recording information	17
4.5	Other Enumeration tools	17

1 INTRODUCTION

1.1 WHAT IS ENUMERATION?

After the footprinting and scanning phases, an attacker will attempt to obtain more detailed information about its intended victim. **Enumeration is an “active” process in which more detailed information about the target is sought.** As such, many of these activities could (and should) be logged by the system administrators. However, that many of these methods would be lost in a “log” as normal behaviour.

Note from experience (!!) that within Abertay, most of these enumeration methods are captured by an Intrusion detection system so please do not try any of them against Abertay.

Much of the information gathered during enumeration may appear harmless, however, once an attacker gains a foothold, such as a valid username or access to a share then it is usually possible to further penetrate the network or system.

The type of information enumerated by intruders:

- Network resources and shares.
- Users and groups.
- E-Mail accounts.
- Policies such as password lockout policies (note that those actually being adopted may be different to the advertised policies).

Enumeration is normally service specific for example DNS Enumeration, NetBIOS Enumeration, Active Directory Enumeration, LDAP Enumeration, SMTP Enumeration, SNMP Enumeration and Firewall Enumeration.

Notes: -

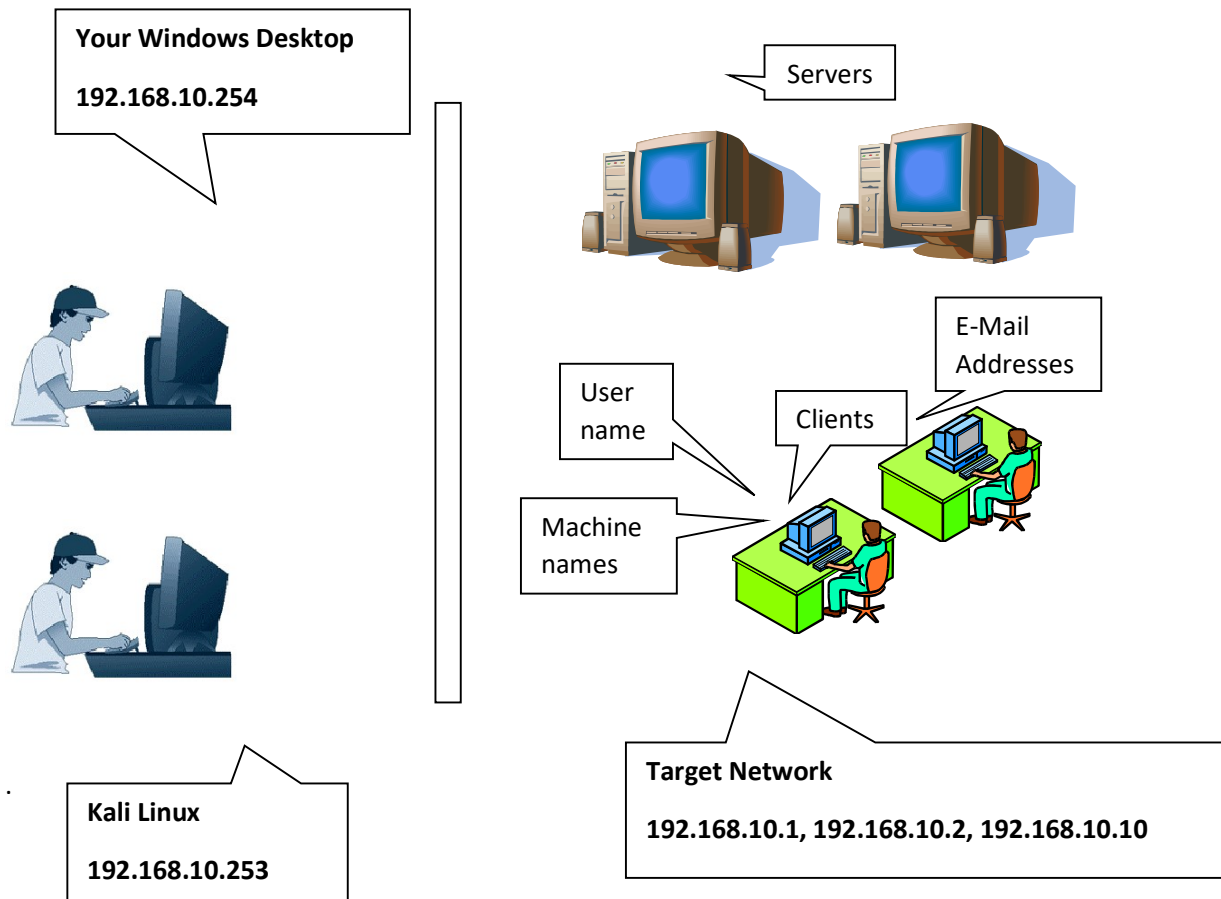
This week contains a lot of different tools that give similar information. Remember that these tools and packages should be evaluated as you complete the exercises.

You can decide what criteria you want to use to evaluate each tool but you may want to consider the following: What would you use the tool for? Which tool would be best for a particular task? What features does the tool have? How does the tool work?

You should take notes of your evaluations for future reference.

1.2 REMINDER OF THE VIRTUAL NETWORK

A diagram of the scenario is shown below. Us as attackers are on the left of the diagram and our target network is on the right: -



i.e. We have a Window machine and a Kali linux machine that we can use to attack the network. Imagine we are sitting in a room within the target company and are about to perform our test. The virtual machines are: -

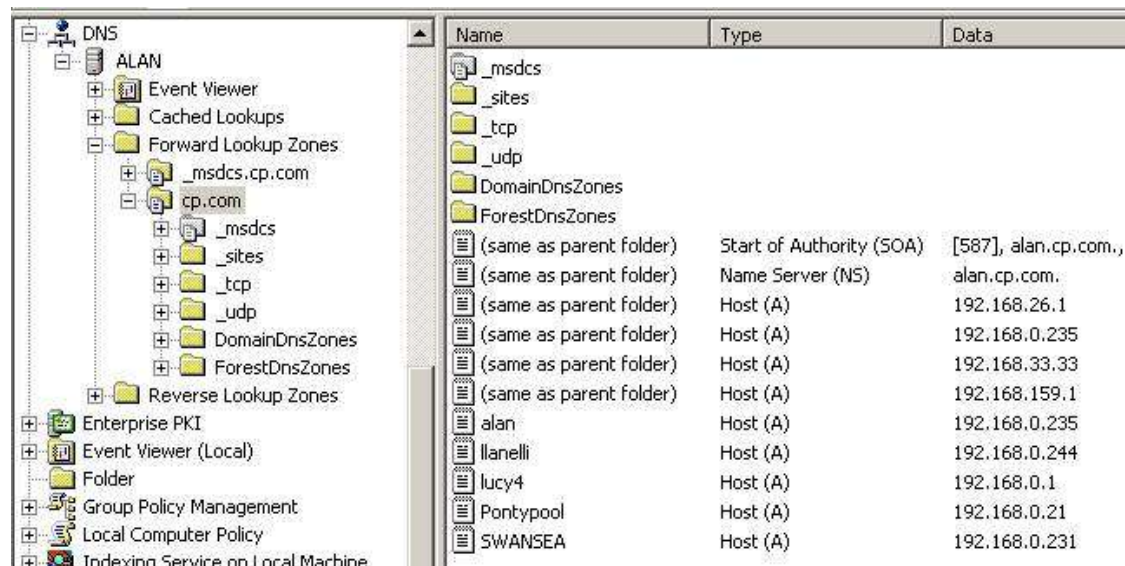
- Tutorial – Server1 = 192.168.10.1
- Tutorial – Server2 = 192.168.10.2
- Tutorial – Client1 = 192.168.10.10
- Kali = 192.168.10.253
- Your main Windows desktop = 192.168.10.254

1.3 RUN THE SERVERS ON THE VIRTUAL NETWORK

- We will interrogate **Server1** and **Server2** so **start BOTH** of these machines from the snapshot **Booted**.

1.4 DNS ENUMERATION.

The basic job of a DNS server is to hold the IP address of a name (e.g. it would hold “www.abertay.ac.uk” is “193.60.160.153”). This is termed a **forward** lookup. A **backward** lookup is the reverse of this. This has been covered in previous lectures (conduct some research to find out information about DNS if you are unsure). A screenshot of the Windows 2008 Server DNS Server snap-in is shown below: -



In the above example, the domain is named ALAN and there are client computers on the network named alan, llanelli, lucy4 etc. Their corresponding IP addresses are 192.168.0.235, 192.168.0.244 etc. Records have different attributes associated with it (see below): -

“A” record

An address (A) record maps a server’s host name to its IP address. There may be many different names associated with an IP address. The A record (address record, or host record) maps a domain name to an IP address on the Internet.

“MX” Record

This record maps the SMTP E-Mail server. When someone sends an E-Mail to xxx@abertay.ac.uk, the IP address for the “abertay.ac.uk” mail server is obtained by searching DNS for the MX record. i.e. what is the server that will deal with E-Mail?

NS

The first resource record in any Domain Name System (DNS) Zone file should be a Start of Authority (SOA) resource record. The SOA resource record indicates that this DNS name server is the best source of information for the data within this DNS domain.

CNAME

CNAME records (Canonical Name records) act as aliases for hostnames. One IP address may have several names (aliases) associated with it. E.g. www.bbc.net.uk and www.bbc.co.uk are the same IP address (212.58.227.78 at this time).

DNS Zone transfers

A DNS transfer will take place from the Primary to the Secondary DNS servers (meaning that the servers should always contain identical records). The transfer will take place at pre-defined intervals. DNS zone transfers have several potential security issues, though they are easily rectified by proper configuration of the DNS software. The data contained in an entire DNS zone may be sensitive in nature. Individually, DNS records are not sensitive, but if a malicious entity obtains a copy of the entire DNS zone for a domain, they may have a complete listing of all hosts in that domain.

An indication that DNS zone transfers are possible is by seeing Port 53 TCP is open (rather than UDP). This was the case from our scans.

Notes: -

- **DNS Zone transfers are TCP (Connection orientated), unlike normal DNS requests which are UDP.**
- Windows Servers are easy to misconfigure, and this misconfiguration is common in networks.

1.5 ANALYSING THE DNS FROM WINDOWS

The nslookup command essentially performs forward and reverse DNS lookups (name to IP address = forward and IP address to name = reverse). The DNS server that is queried can be altered within the command shell using the **server** command.

- From your main Windows desktop, run a command prompt and type:-

nslookup

Manual enumeration is simply a case of typing in the IP address and the name will be returned

- Now set the server to the correct DNS of target network.

server 192.168.10.1

- Then enumerate the DNS names of

192.168.10.1

192.168.10.2

192.168.10.20 (there is no such machine).

192.168.10.25

Note that the names give a clue as to what the machine corresponding to the IP address is and does.

DNS Zone transfers can be attempted

server 192.168.10.1

set type=any

ls -d uadtargetnet.com

If the server has a DNS Zone Transfer Misconfiguration, then it will show all DNS records.

- In the same way, try a Zone transfer from the server **192.168.10.2** (you should find that it's not misconfigured so you should get no information).

1.6 REVERSE DNS

In a similar way, we can try find out information about the network by guessing if a machine name exists. For example, set the server to 192.168.10.1 then try

sales.uadtargetnet.com

email.uadtargetnet.com

1.7 ANALYSING THE DNS FROM KALI LINUX

- Make sure that Kali linux is running.

DNS Zone transfers

A zone transfer can be attempted from Kali linux using the **dig** command (if the server allows zone transfers).

```
dig axfr @192.168.10.1 uadtargetnet.com
```

```
dig axfr @192.168.10.2 uadtargetnet.com
```

or the host command

```
host -t axfr uadtargetnet.com 192.168.10.1
```

```
host -t axfr uadtargetnet.com 192.168.10.2
```

Note that the command **nslookup** is also available from linux

Note the relevance of this.

If we could get the entire DNS for the network (say Abertay University), we could tell by the names what the machines do.

2 NETWORK ENUMERATION USING KALI LINUX

- Ensure that Kali Linux is running.

2.1 SMB ENUMERATION USING NBTSCAN

The Server Message Block protocol (SMB protocol) is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network.

Nbtscan is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network, and is also a first step in finding open shares. The basic command is: -

```
nbtscan 192.168.10.1
```

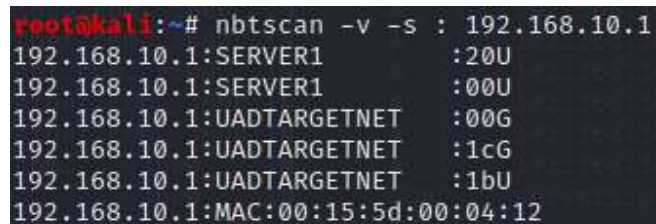
The v switch means verbose.

```
nbtscan 192.168.10.1 -v
```

The following command scans a C-class network. Prints results using the colon as field separator

```
nbtscan -v -s : 192.168.10.1
```

The output should be similar to the following: -

A terminal window screenshot showing the output of the nbtscan command. The prompt is root@kali:~#. The command entered is nbtscan -v -s : 192.168.10.1. The output lists several network resources for 192.168.10.1: SERVER1 (20U, 00U), UADTARGETNET (00G, 1cG, 1bU), and MAC (00:15:5d:00:04:12).

```
root@kali:~# nbtscan -v -s : 192.168.10.1
192.168.10.1:SERVER1      :20U
192.168.10.1:SERVER1      :00U
192.168.10.1:UADTARGETNET :00G
192.168.10.1:UADTARGETNET :1cG
192.168.10.1:UADTARGETNET :1bU
192.168.10.1:MAC:00:15:5d:00:04:12
```

The following link will help you interpret the output from the Remote Machine Name Table that nbtstat has produced for you: -

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961857\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961857(v=technet.10))

2.2 ENUMERATING SHARES USING SMBMAP

A network share is essentially a folder on a machine that can be accessed by others. These shares may be also be folders that a user shares. Juicy information can often be found in these e.g. passwords.txt.

An example from some years ago – a B Sc Ethical Hacking student found a folder that had been accidentally shared initially at home on a lecturers laptop. When they connect to Abertays network, it also shared the folder. It contained their bank account statement.

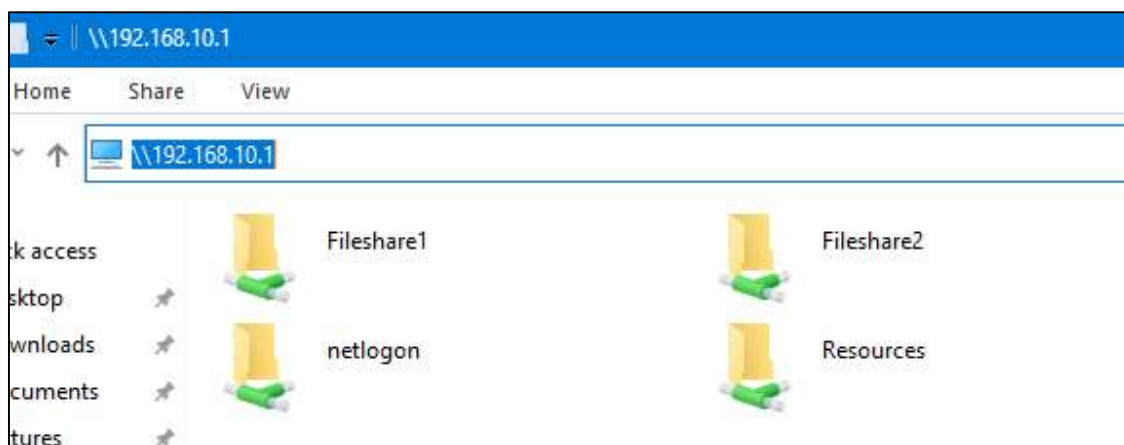
To find the share folders on a machine,

smbmap -u test -p test123 -H 192.168.10.1

```
root@kali:~# smbmap -u test -p test123 -H 192.168.10.1
[+] IP: 192.168.10.1:445      Name: Server1
Disk
-----
ADMIN$      NO ACCESS      Remote Admin
C$          NO ACCESS      Default share
Fileshare1  READ ONLY
Fileshare2  READ ONLY
HR          READ ONLY
IPC$        READ ONLY      Remote IPC
NETLOGON    READ ONLY      Logon server share
Resources   READ ONLY
SYSVOL      READ ONLY      Logon server share
```

Note that the \$ indicates that the share is **not visible** by normal browsing. ADMIN\$, C\$ (C drive), IPC\$ are standard shares created by a Windows machine.

- To prove this, from your main windows desktop, browse the pubic shares on the machine by entering in a folder (use the pen tester account details of **test/test123** when prompted).



- Now examine the shares on Server2 (192.168.10.2).

Reference: -<https://tools.kali.org/information-gathering/smbmap>

2.3 SMB ENUMERATION USING RPCCLIENT

Under Kali linux, RPCclient is an excellent tool for enumerating all aspects of SMB on a Windows network. If we have a valid user account, we can enumerate a lot of information. In this case, use our account details of **test** and a password of **test123**.

- Run the client using: -

```
rpcclient -U "test" 192.168.10.1
```

Try the following useful commands (take notes): -

help

srvinfo

querydominfo

enum then hit TAB twice to show all the enum functions

enumdomusers

enumalsgroups builtin

enumalsgroups domain

lookupnames administrators

lookupnames administrator

A SID (Security Identifier) is a structure of variable length that uniquely identifies an Active directory object in all Windows operating systems. A valid SID looks like the following: -

```
S-1-5-21-8915387-1645822062-181928000-500
```

The final field indicates the RID. The administrator account will always have a RID of 500 (regardless of whether it has been renamed).

The following command will display the Administrator username.

queryuser 500

- At the end, exit rpcclient by typing **exit**

2.4 SMB ENUMERATION USING POLENUM (POLICY ENUMERATOR)

Polenum is a python script which extracts the password policy information on a windows machine. This allows a non-windows (Linux, Mac OSX, BSD etc..) user to query the password policy of a remote windows box without the need to have access to a windows machine.

- Run a terminal in Kali linux and type

polenum test:test123@192.168.10.1

```
[+] Found domain(s):
    [+] UADTARGETNET
    [+] Builtin

[+] Password Info for Domain: UADTARGETNET

    [+] Minimum password length: None
    [+] Password history length: None
    [+] Maximum password age: 136 days 23 hours 58 minutes
    [+] Password Complexity Flags: 010000

        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 1
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0

    [+] Minimum password age: None
    [+] Reset Account Lockout Counter:
    [+] Locked Account Duration:
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: Not Set
```

The “account lockout duration” and Account lockout has not been set. We also have the Minimum Password length as 0 characters. This server clearly has issues!! Also note in real life that the real policy is often different from that advertised.

2.5 SMB ENUMERATION USING ENUM4LINUX

Enum4linux is an excellent tool for enumerating information from Windows and SMB/Samba systems. There are many switches. A full tutorial and an explanation of the switches can be found at <https://labs.portcullis.co.uk/tools/enum4linux/>

- From a terminal, run the following commands and examine the information (ignore any concatenation errors):-

```
enum4linux -U -u test -p test123 192.168.10.1
```

```
enum4linux -G -u test -p test123 192.168.10.1
```

```
enum4linux -S -u test -p test123 192.168.10.1
```

```
enum4linux -a -u test -p test123 192.168.10.1
```

The following line will run all enumerations and takes a few minutes to run.

```
enum4linux -a -u test -p test123 192.168.10.1 >/home/kali/Desktop/enum.txt
```

- Examine the file on the Kali linux desktop and **save for future reference**.

2.6 SMB ENUMERATION USING CRACKMAPEXEC

CrackMapExec (a.k.a CME) is a post-exploitation tool that helps automate assessing the security of *large* Active Directory networks. It has a lot of functionality and we will use it in future weeks. To get basic help,

```
crackmapexec smb --help
```

The syntax for obtaining the users is: -

```
crackmapexec smb 192.168.10.1 -u 'test' -p 'test123' --users
```

- Also, try the following switches.
- | | |
|-------------------|-----------------------------|
| --shares | enumerate shares and access |
| --sessions | enumerate active sessions |
| --disks | enumerate disks |
| --groups | enumerate domain groups |
| --pass-pol | dump password policy |

3 OTHER ENUMERATION TECHNIQUES

3.1 SNMP ENUMERATION FROM KALI LINUX

One of the most common enumeration techniques is via SNMP (Simple Network Management Protocol). This protocol runs on routers, switches, firewalls and other network devices. It is also common for the protocol to run on servers (E.g. Windows 2018 Server). Note that SNMP can be enumerated from anywhere on the Internet (if misconfigured). SNMP is perhaps **the** most common misconfigured protocol that is used for enumeration.

There are two community names commonly used (mostly by default): -

- Private (Read-write access)
- Public (Read only access).

Enumerating systems via the SNMP public community string gives a lot of useful information. For reference, on a Windows system – some of the MIB variables can be found in the following places: -

RUNNING PROCESSES	1.3.6.1.2.1.25.4.2.1.2
INSTALLED SOFTWARE	1.3.6.1.2.1.25.6.3.1.2
SYSTEM INFO	1.3.6.1.2.1.1.1
HOSTNAME	1.3.6.1.2.1.1.5
DOMAIN	1.3.6.1.4.1.77.1.4.1
UPTIME	1.3.6.1.2.1.1.3
USERS	1.3.6.1.4.1.77.1.2.25
SHARES	1.3.6.1.4.1.77.1.2.27
DISKS	1.3.6.1.2.1.25.2.3.1.3
SERVICES	1.3.6.1.4.1.77.1.2.3.1.1
LISTENING TCP PORTS	1.3.6.1.2.1.6.13.1.3.0.0.0.0
LISTENING UDP PORTS	1.3.6.1.2.1.7.5.1.2.0.0.0.0

On a Linux system: -

RUNNING PROCESSES	1.3.6.1.2.1.25.4.2.1.2
SYSTEM INFO	1.3.6.1.2.1.1.1

HOSTNAME	1.3.6.1.2.1.1.5
MOUNTPPOINTS	1.3.6.1.2.1.25.2.3.1.3
RUNNING SOFTWARE PATHS	1.3.6.1.2.1.25.4.2.1.4
LISTENING UDP PORTS	1.3.6.1.2.1.7.5.1.2.0.0.0.0
LISTENING TCP PORTS	1.3.6.1.2.1.6.13.1.3.0.0.0.0

Snmpcheck under Kali linux allows you to enumerate the useful SNMP devices and places the output in a human readable friendly format.

Note: - You will only get output IF the public string is enabled.

- Run the tool against the servers to see if they are vulnerable.

snmp-check -c public 192.168.10.1

snmp-check -c public 192.168.10.2

- Examine the information gained (if you got anything).

3.2 SMTP ENUMERATION FROM KALI LINUX

Several methods exist that can be used to abuse SMTP to enumerate valid E-Mails and addresses, namely VRFY, EXPN, and RCPT TO. The procedure consists of trying potentially valid e-mail addresses. This can be made easier using Google Hacking to find potential E-mail addresses or by previous enumeration methods.

From Linux, we could create a file of potentially valid usernames and use **smtp-user-enum** to test. To prove the concept, we will try a single user to see if their e-mail exists.

- Under Kali Linux, type the following from a terminal.

smtp-user-enum -M RCPT -u A.George -t 192.168.10.1

You should see from the output that the user A.George exists.

```
target domain .....
##### Scan started at Tue Ju
192.168.10.1: A.George exists
##### Scan completed at Tue
```

4 ENUMERATION USING WINDOWS.

4.1 NBTENUM3.3

There are several NetBIOS enumeration tools that can be used but nbtenum3.3 gives an excellent formatted web page output. A valid user account is required (in our case, test/test123). On your main Windows machine, we will attempt to enumerate via netbios using NBTenum3.3.

- Run a command prompt in the **tools\NBTEnum33** folder and run the scan against Server1

nbtenum.exe -q 192.168.10.1 192.168.10.1\test test123

- This creates a file **192.168.10.1.html** in the nbtenum3.3 folder. Examine this file.
- Also, save this file for later use.

4.2 NETBIOS ENUMERATION USING NBTSTAT

Note that some tools will only work if you are a logged in member of the domain. We will now log on to the domain from **Client1** and use these tools to enumerate.

- **Close the virtual machines Server 2 and Kali Linux.**
- **Restore the Client1 virtual machine from the snapshot booted. You are logged in to the domain as test (password is test123).**

There are several in-built commands within Windows that allow us to enumerate. These can be useful if you are part of a domain and you can't install tools easily.

nbtstat is a Windows diagnostic tool for NetBIOS over TCP/IP. It is included in several versions of Microsoft Windows. Its primary design is to help troubleshoot NetBIOS name resolution problems.

- **ON CLIENT1**, From a command prompt under Windows, type

nbtstat -A 192.168.10.1

NetBIOS Remote Machine Name Table			
Name		Type	Status
SERVER1	<00>	UNIQUE	Registered
UADTARGETNET	<00>	GROUP	Registered
UADTARGETNET	<1C>	GROUP	Registered
SERVER1	<20>	UNIQUE	Registered
UADTARGETNET	<1B>	UNIQUE	Registered
MAC Address = 00-0C-29-25-86-06			

Again, the output can be deciphered using [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961857\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961857(v=technet.10))

- To view shares, type

net view \\192.168.10.1 /All

- Try the following useful commands: -

net user /domain

net user A.George /domain

wmic useraccount

net group "Domain Computers" /domain

net group "Domain Controllers" /domain

4.3 SID2USER/USER2SID

A SID (Security Identifier) is a structure of variable length that uniquely identifies an Active directory object in all Windows. A valid SID looks like the following: -

S-1-5-21-8915387-1645822062-181928000-500

Browse the following article (it shows the structure of a SID).

- <http://support.microsoft.com/kb/q243330/>

The last number is particularly important to a hacker. The number for an Administrator is always **500**, Guest is **501**, "domain users" is always **513**. The last group will **always** exist.

It is common for a sysadmin to rename the Administrator account to try and hide it from attackers. The packages user2sid and sid2user can be used in the following way to show the user name: -

```
C:\>net use \\99.99.99.99\IPC$ "" /u:""
```

```
C:\>User2sid \\99.99.99.99 "domain users"
```

This gives an output similar to the following: -

```
S-1-5-21-8915387-1645822062-181928000-513
```

```
Number of subauthorities is 5
```

```
Domain is TESTDOMAIN
```

Length of SID in memory is 28 bytes

Type of SID is SidTypeGroup

Now we want to know the Administrator's account name. We add in the SID with a **500** at the end (instead of a **513**).

```
C:\>sid2user \\99.99.99.99 5 21 8915387 1645822062 181928000 500
```

The files user2sid.exe and sid2user.exe are in C:\Users\student\Desktop\tools on your Azure machine.

- **Shut down Client1.**
- Run the following exercise from your main Windows desktop

We will now create a session as our valid user (credentials **test/test123**)

- Run a command prompt from the tools folder.

net use \\192.168.10.1\resources

enter username as test
enter password as test123

user2sid.exe \\192.168.10.1 "domain users"

Note:- You need to know the name of a **valid sharename** (rather than user\$) if you are not on a machine connected to the domain.

- **Challenge:** - Now use **sid2user** to get the name of the administrator and the guest. **(You will need to look at the syntax in the explanation above and be careful of dashes and spaces).**

RESEARCH EXERCISES

4.4 RECORDING INFORMATION

Have a thought about your coursework. How are you going to record all this information? Are you going to use a spreadsheet or a word document? What information are you going to record?

4.5 OTHER ENUMERATION TOOLS

There are various enumeration protocol packages that have been written by 3rd parties and are on github. One example is Swaks

<http://www.jetmore.org/john/code/swaks/latest/doc/ref.txt>

There are also tools that have made available by pen testing companies. E.g. NCCgroup.

https://github.com/nccgroup/ssh_user_enum