ETHICAL HACKING V2
LAB SERIES

Lab 20: Enumeration

Document Version: 2021-05-18

Material in this Lab Aligns to the Following	
Books/Certifications	**Chapters/Modules/Objectives**
All-In-One CEH Chapters ISBN-13: 978-1260454550	3: Scanning and Enumeration 4: Sniffing and Evasion
EC-Council CEH v10 Domain Modules	4: Enumeration

Contents

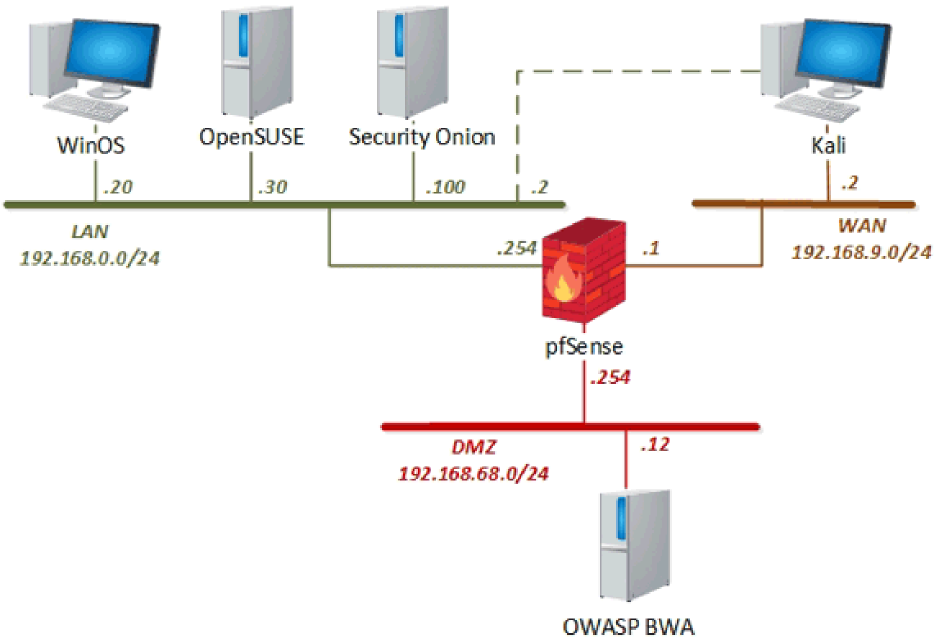
Introduction

Enumeration is the systematic collection of system information for identification purposes. Penetration Testers examine systems in their entirety to evaluate the security weaknesses.

Objectives

- Performing NetBIOS Enumerator Enumeration using NMAP
- List computers, their Operating System, and ports
- Enumerating network using SuperScan
- LDAP Enumeration

Lab Topology



Lab Settings

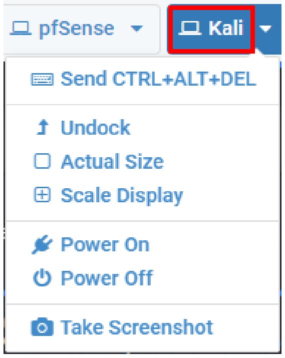
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address / Subnet Mask	Account (if needed)	Password (if needed)
WinOS	192.168.0.20	Administrator	Train1ng$
Kali Linux	192.168.9.2 192.168.0.2	root	toor
OWASP BWA	192.168.68.12	root	owaspbwa

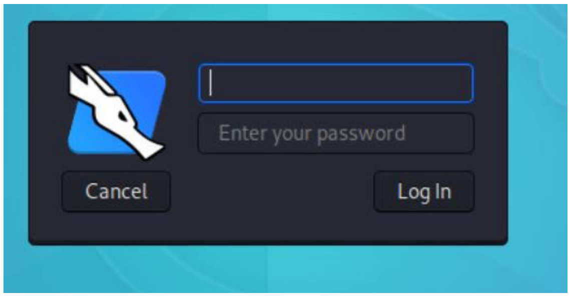
1 Enumeration Services on a Target Machine

Enumeration is the process in which information from individual systems is methodically collected and identified. Penetration Testers examine systems in their entirety to evaluate the security weaknesses. In this exercise, we will enumerate all the services running on the port, along with their respective versions.

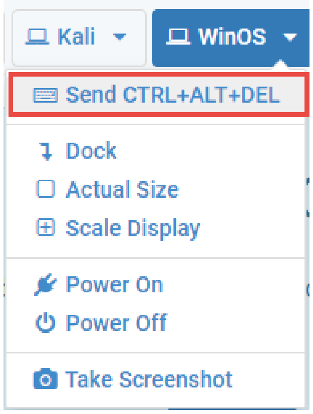
1. To begin, launch the **Kali Linux** virtual machine to access the graphical login screen.



2. Log in as `root` using the password: `toor`

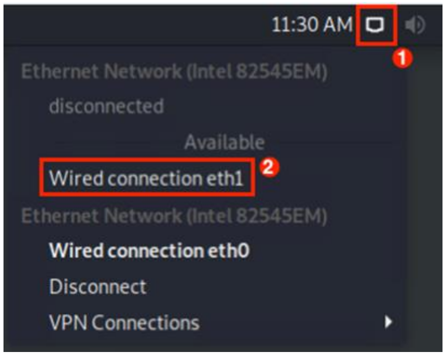


3. Launch the **WinOS** to access the graphical login screen. This will be the target machine.
   3.1. Select **Send CTRL+ALT+DEL** from the dropdown menu to be prompted with the login screen.



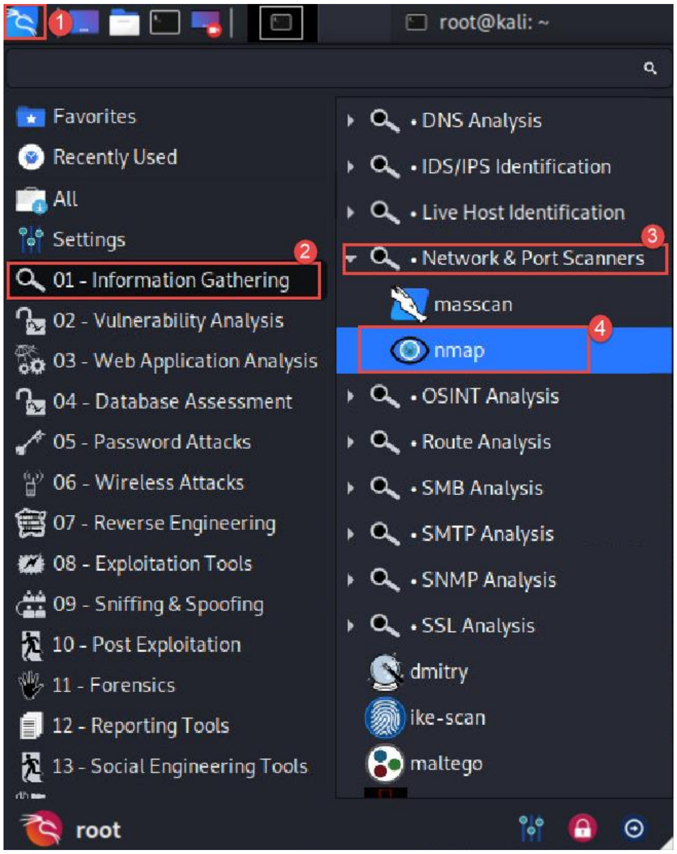
   3.2. Log in as `Administrator` using the password: `Train1ng$`

4. Now, let us switch back to the Kali machine. Before starting the lab, ensure that the host machine is on the same network as the target machine. Select the **Ethernet network connection** from the navigation panel, as seen in *item* **1**. Then, click **Wired connection eth1** to allow *Kali Linux* to use the interface with the IP address 192.168.0.2, as seen in *item* **2**.

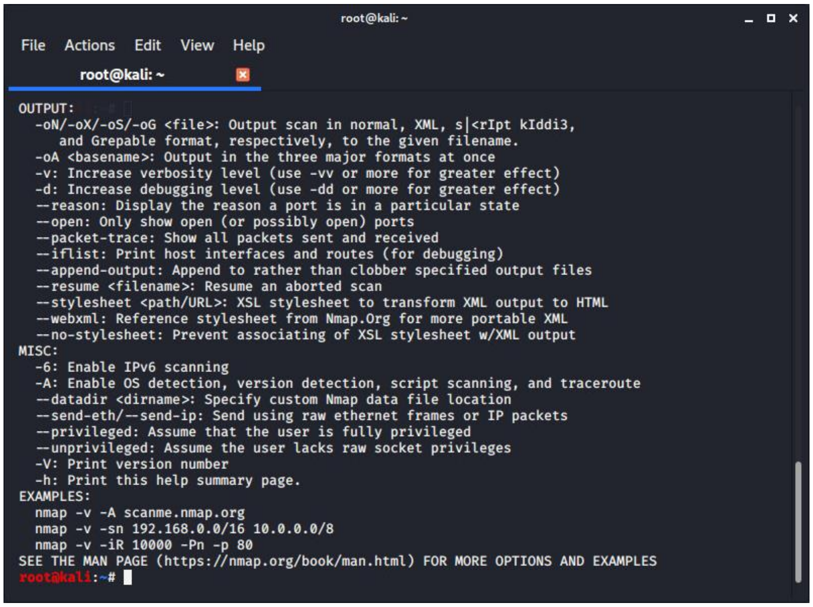


STOP The target machine is on the network 192.168.0.0/24. The Kali Linux VM is configured with both IP addresses and can be easily interchanged.

5. Let us start by launching **nmap.** To do this, navigate to **Whisker Menu** > **Information Gathering** > **Network & Port Scanners** > **nmap** as seen in *items* **1**, **2**, **3,** and **4** below.



6. Once started, the Nmap application will appear in a command line terminal, displaying all the switches that can be used to perform scanning.

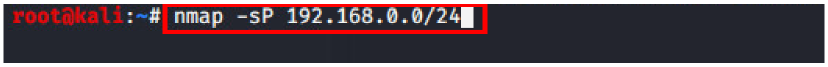


```
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# 
```

Review the instructions/switches to become more familiar with the tool.

7. Now, type **nmap -sP** <***IP address of the target subnet***> then press **Enter.** The target subnet will be **192.168.0.0/24**.

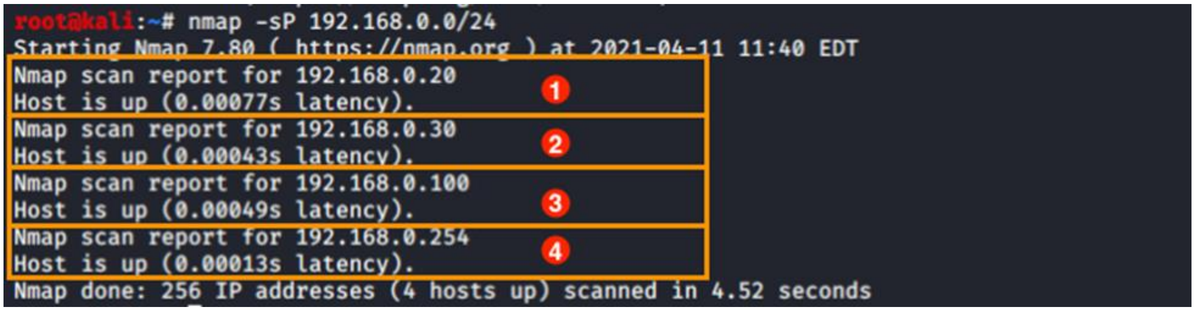
```
root@kali:~# nmap -sP 192.168.0.0/24
```



```
root@kali:~# nmap -sP 192.168.0.0/24
```

-sP means Ping Sweep scan, the result will list the hosts within the specific range that responded to a ping. More details can be viewed under Scan Techniques/Types.

8. Nmap scans all nodes on the given network range and displays all active hosts. Let us see the results from the subnet 192.168.0.0/24. It appears that IP addresses **.20 .30 .100,** and **.254** are active, as seen at *items* **1**, **2**, **3,** and **4** below.



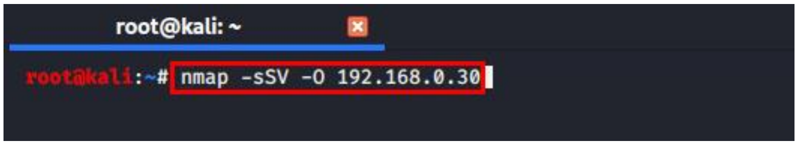
```
root@kali:~# nmap -sP 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-11 11:40 EDT
Nmap scan report for 192.168.0.20
Host is up (0.00077s latency).
Nmap scan report for 192.168.0.30
Host is up (0.00043s latency).
Nmap scan report for 192.168.0.100
Host is up (0.00049s latency).
Nmap scan report for 192.168.0.254
Host is up (0.00013s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 4.52 seconds
```

The IP address **192.168.0.2** is the Kali Linux host and will not be included in the list, however, it is a part of this subnet.

9. Great, there are four (4) active hosts on the network. Now that we obtained open ports, along with the services running, we can now attempt to enumerate the versions of each running service on the ports by performing a SYN scan with the version detection switch enabled.

10. Type `nmap -sSV -O` *<IP address of the target subnet>* then press **Enter.** The IP address used in this lab is **192.168.0.30.**

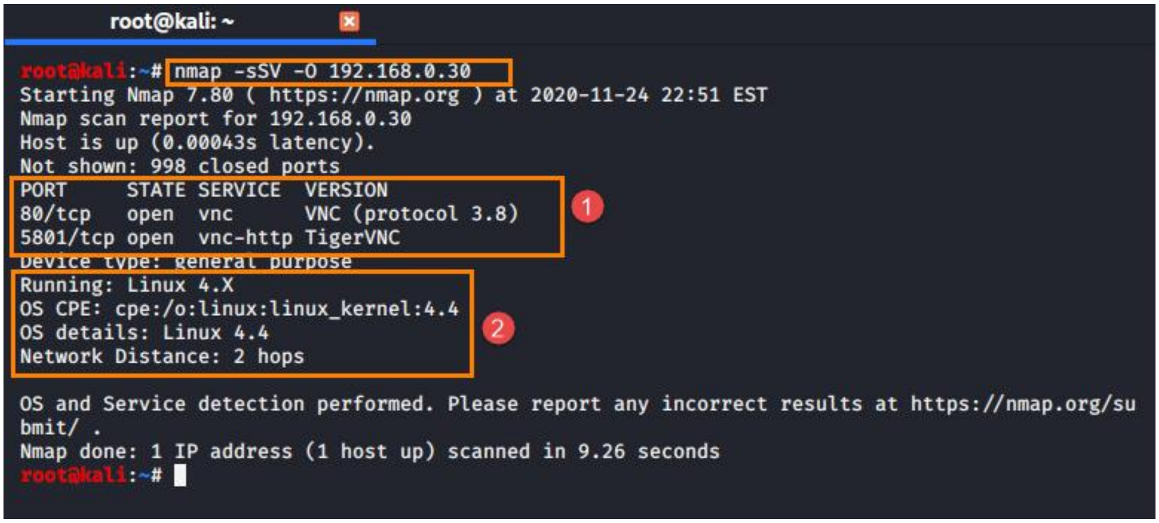
```
root@kali:~# nmap -sSV -O 192.168.0.30
```



```
root@kali:~# nmap -sSV -O 192.168.0.30
```

This command initiates a stealthy SYN scan with version detection along with OS detection. Version detection collects information about the specific service running on an open port, including the product name and version number.

11. NMAP performs the scan and displays the versions of the services, along with the OS fingerprint, as seen in *items* **1** and **2** below.



```
root@kali:~# nmap -sSV -O 192.168.0.30
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-24 22:51 EST
Nmap scan report for 192.168.0.30
Host is up (0.00043s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE   VERSION
80/tcp    open  vnc       VNC (protocol 3.8)
5801/tcp open  vnc-http TigerVNC
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.26 seconds
root@kali:~#
```

12. Change the target IP address as identified in step 9 and repeat the process to identify the remaining active hosts.

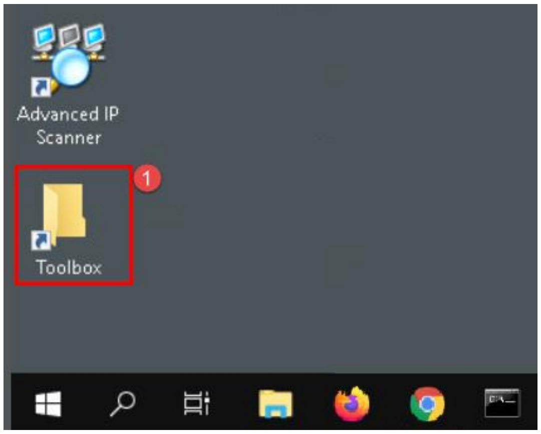
    a. Type `nmap -sSV -O 192.168.0.20` and then press **Enter**.
    b. Type `nmap -sSV -O 192.168.0.100` and then press **Enter**.
    c. Type `nmap -sSV -O 192.168.0.254` and then press **Enter**.

13. By performing services enumeration, we are now able to research vulnerability associated with that particular application and exploit them to gain access to the target machine.

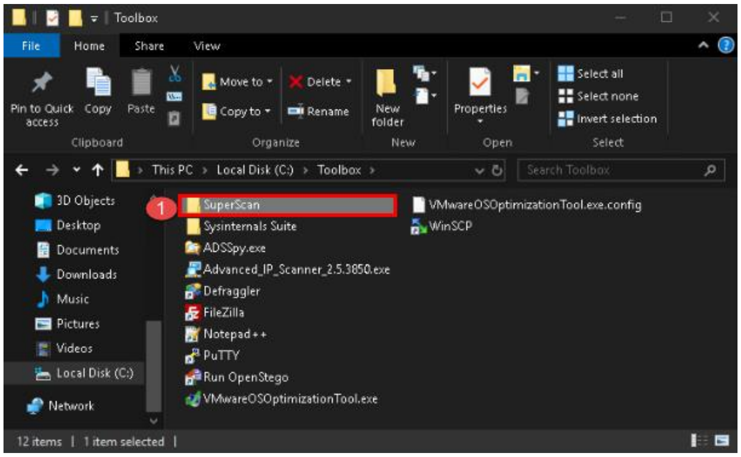
2 Enumerating a Network Using SuperScan

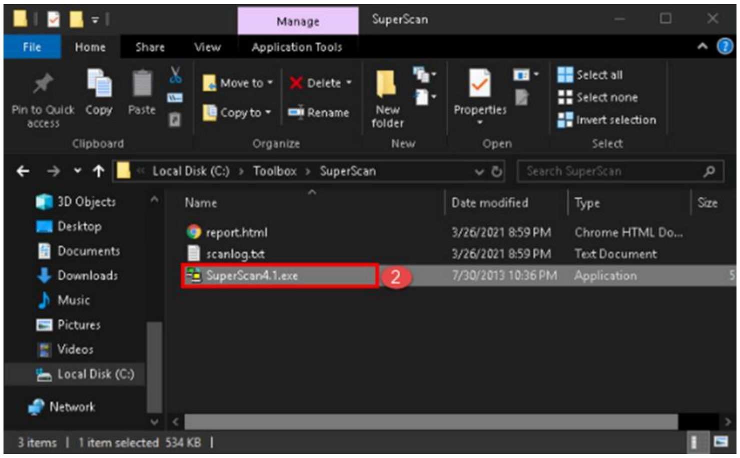
Enumeration is the systematic collection of network information to identify a system. It is important that a penetration tester examine the targeted system in its entirety to evaluate security vulnerabilities. In this lab. We will extract NetBIOS information, group and user accounts, network shares, and services.

1. Switch back to the Windows VM. Navigate to and double-click the **Toolbox** directory located on the desktop, as seen in *item* **1** below.



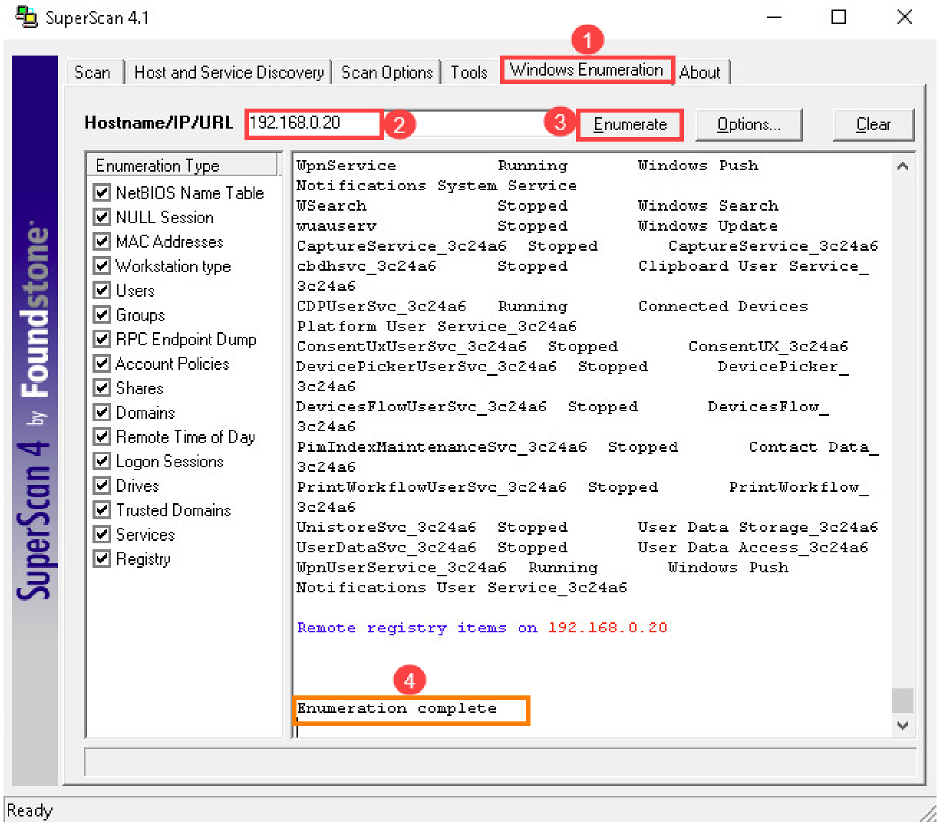
2. In *Windows File Explorer*, double-click the folder **SuperScan** and double-click **SuperScan4.1.exe** to launch the application as highlighted in *items* **1** and **2**.


Toolbox
File
Home
Share
View
This PC > Local Disk (C:) > Toolbox >
Search Toolbox
1
SuperScan
Sysinternals Suite
ADSSpy.exe
Advanced_IP_Scanner_2.5.3850.exe
Defraggler
FileZilla
Notepad++
PuTTY
Run OpenStego
VMwareOSOptimizationTool.exe
VMwareOSOptimizationTool.exe.config
WinSCP
12 items | 1 item selected |



If prompted by the User Access Control, click **Run.**

3. The *SuperScan* window will appear, it has a simple-looking interface that allows you to gather some useful information about the target systems on the network. First, let us click on the Windows Enumeration tab, as seen in *item* **1**. Next, enter the IP address `192.168.0.20` of the target machine in the *Hostname/IP/URL* textbox and click **Enumerate** as seen in *item* **2** and **3** below. SuperScan will start enumerating the provided target and displays the results. After the scan is completed, a message will be displayed at the end of the enumeration results, as seen in *item* **4** below.



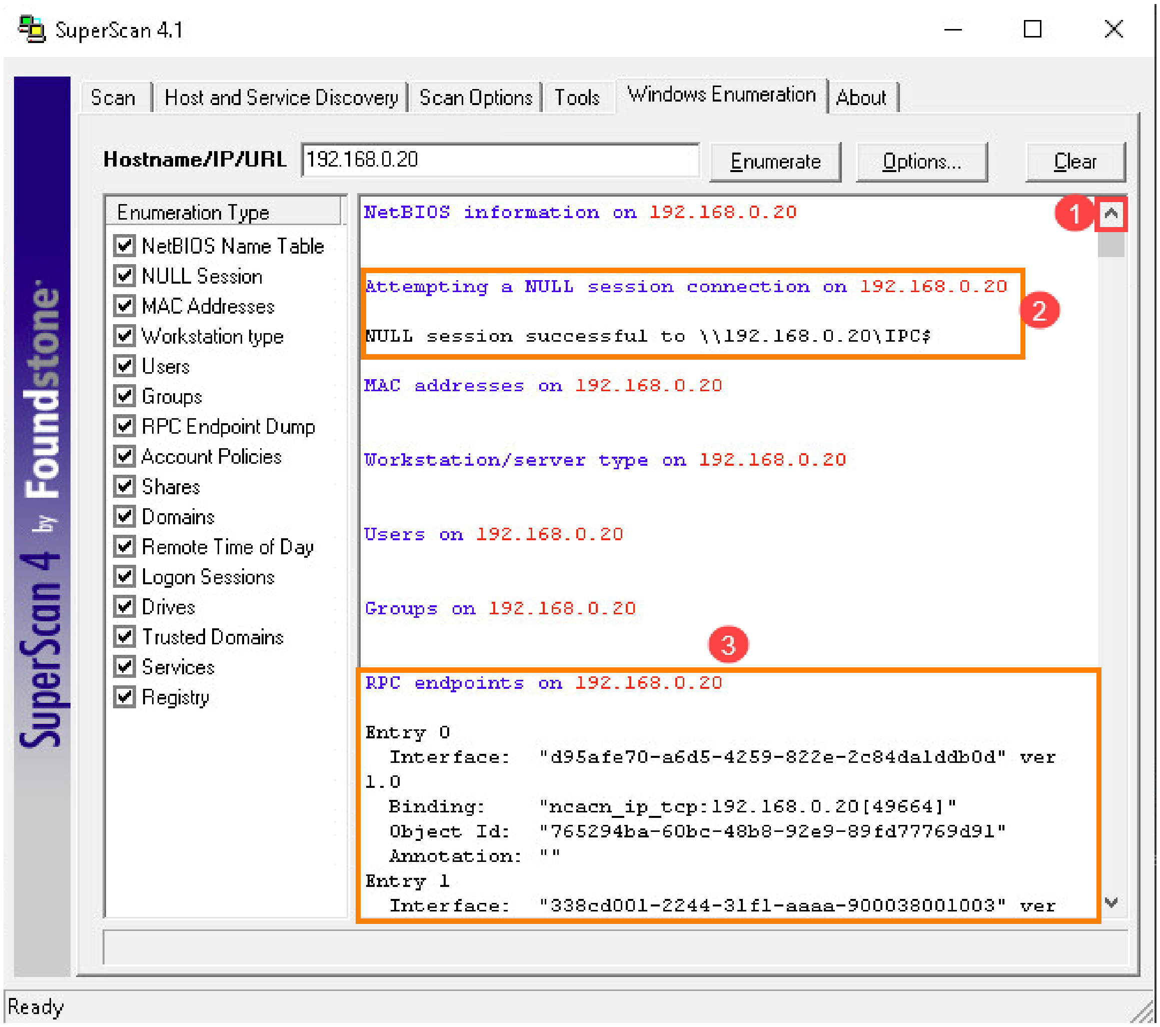
Hostname/IP/URL 192.168.0.20

Enumeration Type
- ☑ NetBIOS Name Table
- ☑ NULL Session
- ☑ MAC Addresses
- ☑ Workstation type
- ☑ Users
- ☑ Groups
- ☑ RPC Endpoint Dump
- ☑ Account Policies
- ☑ Shares
- ☑ Domains
- ☑ Remote Time of Day
- ☑ Logon Sessions
- ☑ Drives
- ☑ Trusted Domains
- ☑ Services
- ☑ Registry

```
WpnService          Running       Windows Push
Notifications System Service
WSearch             Stopped       Windows Search
wuauserv            Stopped       Windows Update
CaptureService_3c24a6  Stopped       CaptureService_3c24a6
cbdhsvc_3c24a6      Stopped       Clipboard User Service_
3c24a6
CDPUserSvc_3c24a6   Running       Connected Devices
Platform User Service_3c24a6
ConsentUxUserSvc_3c24a6  Stopped       ConsentUX_3c24a6
DevicePickerUserSvc_3c24a6  Stopped       DevicePicker_
3c24a6
DevicesFlowUserSvc_3c24a6  Stopped       DevicesFlow_
3c24a6
PimIndexMaintenanceSvc_3c24a6  Stopped       Contact Data_
3c24a6
PrintWorkflowUserSvc_3c24a6  Stopped       PrintWorkflow_
3c24a6
UnistoreSvc_3c24a6  Stopped       User Data Storage_3c24a6
UserDataSvc_3c24a6  Stopped       User Data Access_3c24a6
WpnUserService_3c24a6  Running       Windows Push
Notifications User Service_3c24a6

Remote registry items on 192.168.0.20


Enumeration complete
```

By default, the Enumeration types are selected. We can leave it as is to obtain all the information we can.

4. Now, scroll the window as seen in *item* **1** to see the results of the enumeration. As you can see from the results, the Windows VM is vulnerable to a null session attack, as seen in *item* **2**. At *item* **3,** you will see records from a Remote Procedure Calls (RPC) endpoint. RPC endpoint is a network-specific address of a server process, using an RPC endpoint mapper an attacker can establish a TCP/IP connection and use it to determine the port number currently assigned to the service. However, that will not be covered in this lab.

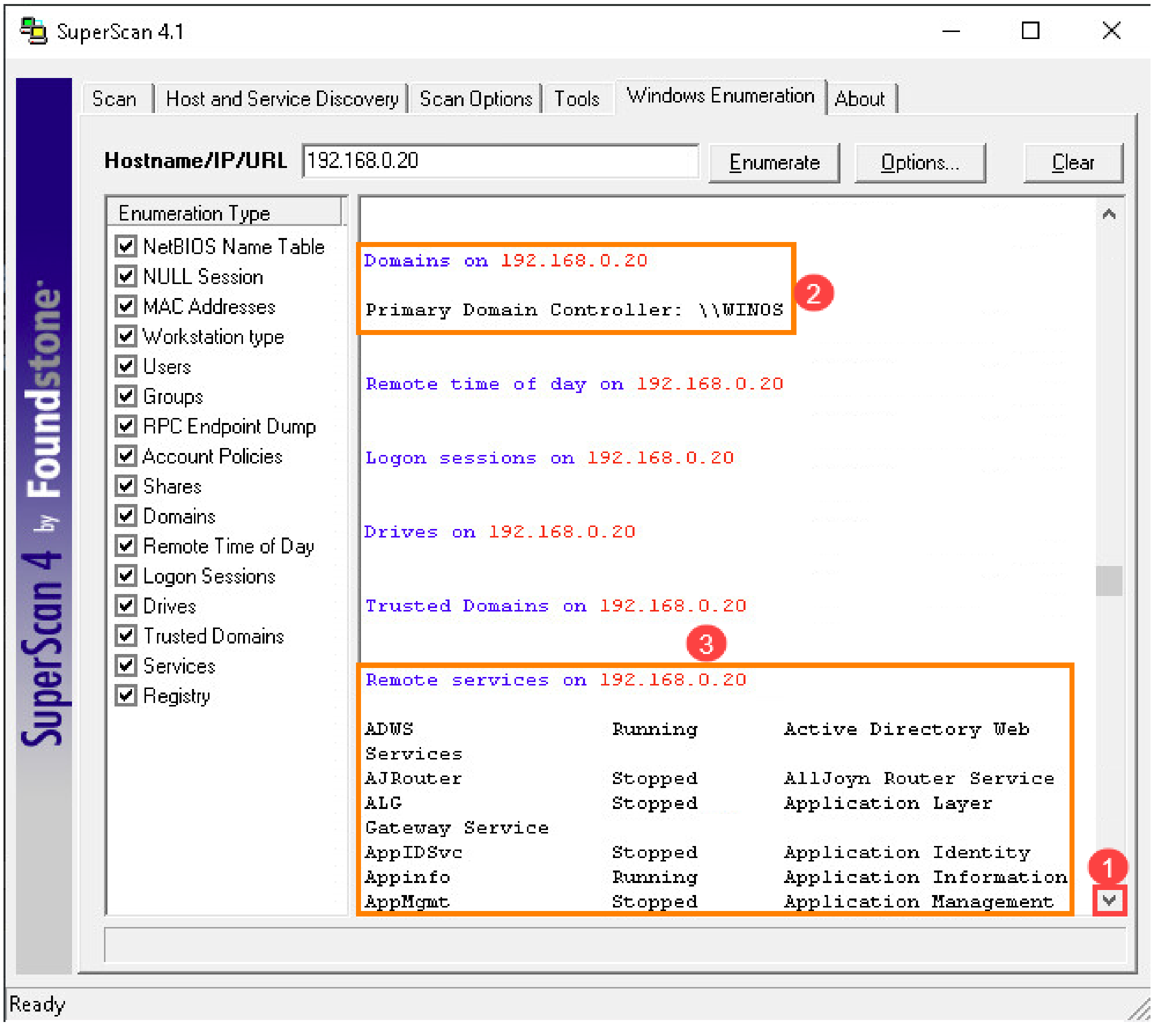


Hostname/IP/URL 192.168.0.20

Enumeration Type
- ☑ NetBIOS Name Table
- ☑ NULL Session
- ☑ MAC Addresses
- ☑ Workstation type
- ☑ Users
- ☑ Groups
- ☑ RPC Endpoint Dump
- ☑ Account Policies
- ☑ Shares
- ☑ Domains
- ☑ Remote Time of Day
- ☑ Logon Sessions
- ☑ Drives
- ☑ Trusted Domains
- ☑ Services
- ☑ Registry

```
NetBIOS information on 192.168.0.20


Attempting a NULL session connection on 192.168.0.20

NULL session successful to \\192.168.0.20\IPC$

MAC addresses on 192.168.0.20


Workstation/server type on 192.168.0.20


Users on 192.168.0.20


Groups on 192.168.0.20


RPC endpoints on 192.168.0.20

Entry 0
  Interface:   "d95afe70-a6d5-4259-822e-2c84da1ddb0d" ver
1.0
  Binding:     "ncacn_ip_tcp:192.168.0.20[49664]"
  Object Id:   "765294ba-60bc-48b8-92e9-89fd77769d91"
  Annotation:  ""
Entry 1
  Interface:   "338cd001-2244-31f1-aaaa-900038001003" ver
```

5. Now, scroll the window until you locate ***Domains on 192.168.0.20***, as seen in *item* **1**. Here SuperScan identified that WINOS as the Primary Domain Controller seen in *item* **2** and a list of remote services both stopped and running as seen in *item* 3.



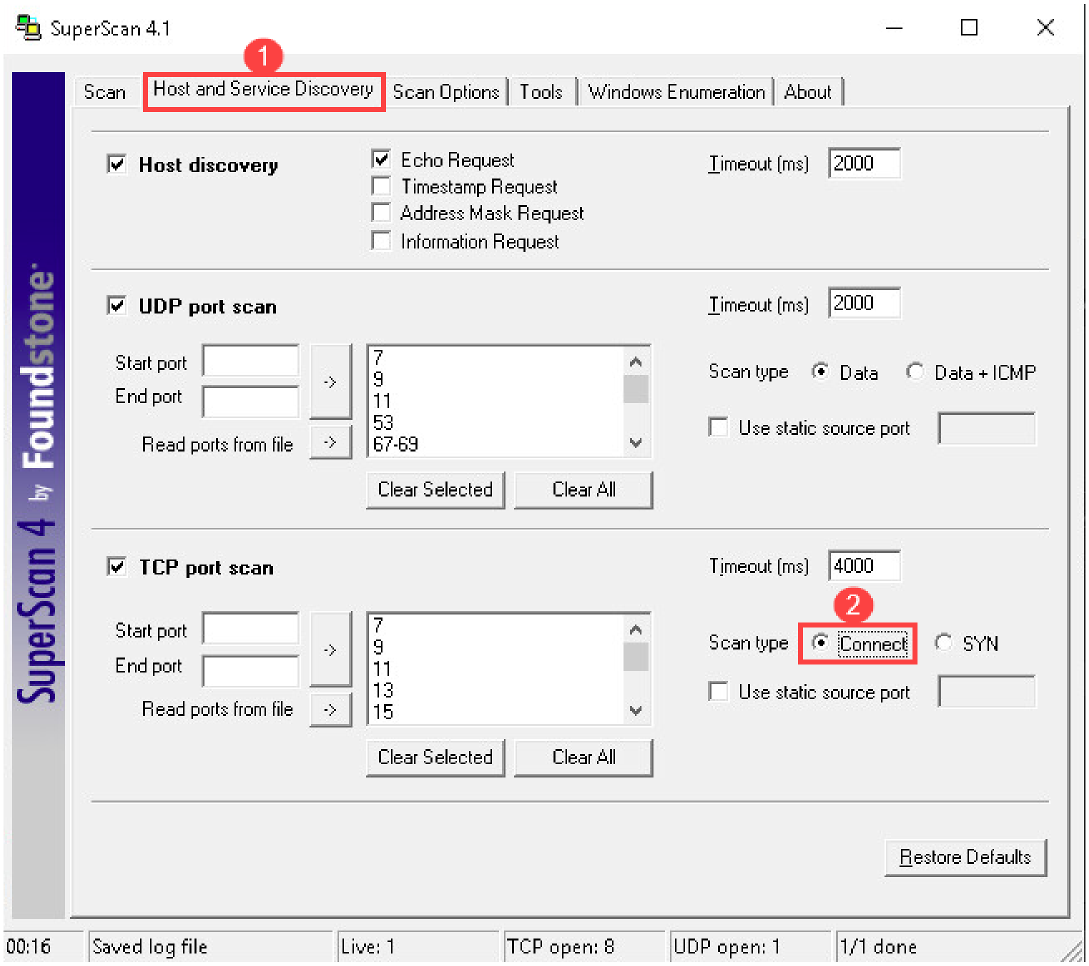
Hostname/IP/URL 192.168.0.20

☑ NetBIOS Name Table
☑ NULL Session
☑ MAC Addresses
☑ Workstation type
☑ Users
☑ Groups
☑ RPC Endpoint Dump
☑ Account Policies
☑ Shares
☑ Domains
☑ Remote Time of Day
☑ Logon Sessions
☑ Drives
☑ Trusted Domains
☑ Services
☑ Registry

```
Domains on 192.168.0.20

Primary Domain Controller: \\WINOS


Remote time of day on 192.168.0.20


Logon sessions on 192.168.0.20


Drives on 192.168.0.20


Trusted Domains on 192.168.0.20


Remote services on 192.168.0.20

ADWS                 Running       Active Directory Web
Services
AJRouter             Stopped       AllJoyn Router Service
ALG                  Stopped       Application Layer
Gateway Service
AppIDSvc             Stopped       Application Identity
Appinfo              Running       Application Information
AppMgmt              Stopped       Application Management
```

Additional information can be gleaned from the enumeration scan. Please feel free to review the results further.

6. The previous enumeration scan was specific to Windows. Let us try to perform a new enumeration scan against a Linux host. Before we go ahead, click on the **Host and Service Discovery** tab seen in *item* **1**. Once there, click the **Connect** radio button as seen in *item* **2** to change the scan type from a SYN (half-open/stealth) scan to a TCP connect scan.



SuperScan 4.1

☑ Host discovery

☑ Echo Request
☐ Timestamp Request
☐ Address Mask Request
☐ Information Request

Timeout (ms) 2000

☑ UDP port scan

Start port
End port
Read ports from file

7
9
11
53
67-69

Timeout (ms) 2000

Scan type ● Data ○ Data + ICMP

☐ Use static source port

☑ TCP port scan

Start port
End port
Read ports from file

7
9
11
13
15

Timeout (ms) 4000

Scan type ● Connect ○ SYN

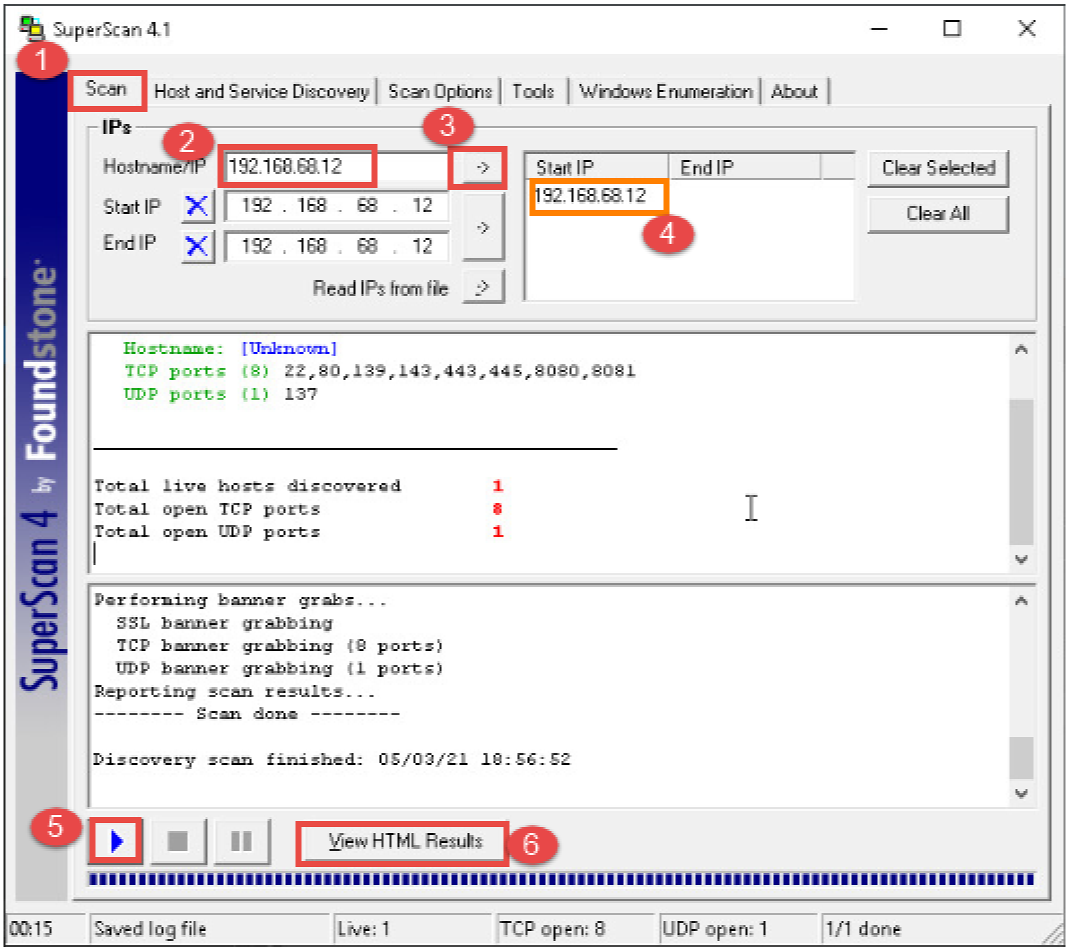
☐ Use static source port

00:16 | Saved log file | Live: 1 | TCP open: 8 | UDP open: 1 | 1/1 done

The *TCP connect scan* attempts to perform a full 3-way handshake with the target ports and determines whether a port is open based on the response.

A *SYN (half-open/stealth) scan* does not perform the full 3-way handshake and is used to evade older intrusion detection systems. Some applications listening on the target ports may not capture the attempted connection from SYN scans as well, since it was not a complete connection. For this purpose, it is considered a stealthier scan than a TCP connect scan.

7. Now, let us set up and run the scan. To do this, click on the **Scan** tab as seen in *item* **1**. Next, enter the IP address **`192.168.68.12`** of the target machine in the *Hostname/IP/URL* textbox and click the import arrow to insert the target IP address under the *Start IP* column, as seen in *items* **3** and **4.** Now click the **Start** button located at the bottom-left corner of the application to initiate the Enumeration scan, as seen in *item* **5.** At the end of the scan, the **View HTML Results** will become visible**;** click this to see the results in a web browser, as seen in *item* **6** below.



Hostname/IP: 192.168.68.12

Start IP: 192 . 168 . 68 . 12

End IP: 192 . 168 . 68 . 12

Start IP	End IP
192.168.68.12	

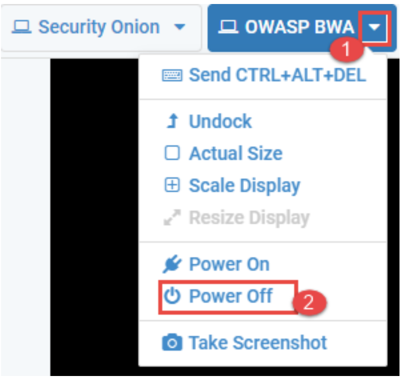
```
   Hostname: [Unknown]
   TCP ports (8) 22,80,139,143,443,445,8080,8081
   UDP ports (1) 137

____________________________________________

Total live hosts discovered        1
Total open TCP ports               8
Total open UDP ports               1
```

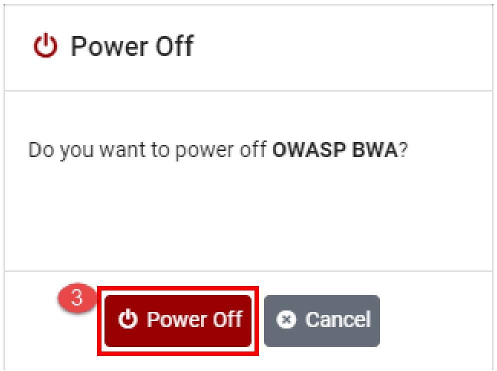
```
Performing banner grabs...
  SSL banner grabbing
  TCP banner grabbing (8 ports)
  UDP banner grabbing (1 ports)
Reporting scan results...
-------- Scan done --------

Discovery scan finished: 05/03/21 18:56:52
```

```
00:15 | Saved log file | Live: 1 | TCP open: 8 | UDP open: 1 | 1/1 done
```

If your scan did not identify a UDP port, please proceed to step 8 below. Otherwise continue to step 10.

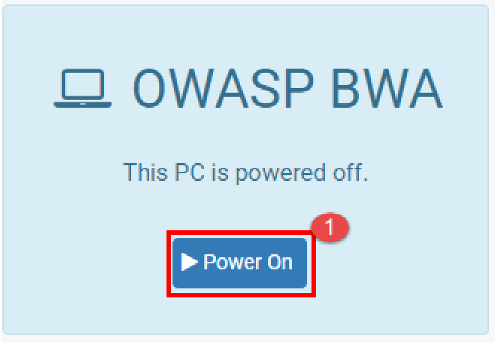
8. **Optional:** Let us reboot the OWASP BWA machine and try running the scan again. Select the dropdown arrow beside OWASP BWA machine. Then click **Power Off** as seen in *items* **1** and **2**. If prompted for confirmation, click **Power OFF,** as seen in *item* **3** below.





Do you want to power off **OWASP BWA**?

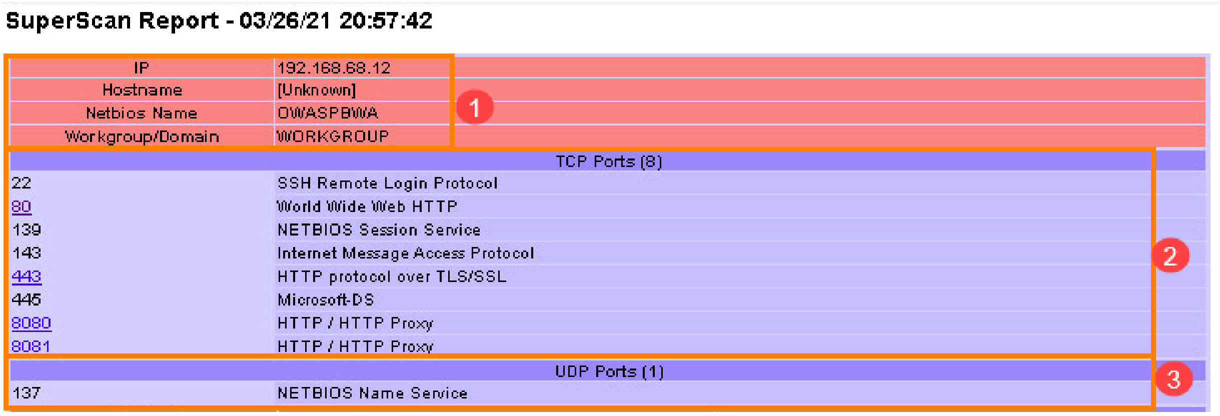
9. **Optional:** Now, start the machine by clicking **Power On** as seen in *item* **1** below. After the OWASP BWA machine has successfully started, try running the scan again from the WinOS VM and observe the results.



This PC is powered off.

If your scan identified a UDP port after the reboot, please proceed to step 10 below.

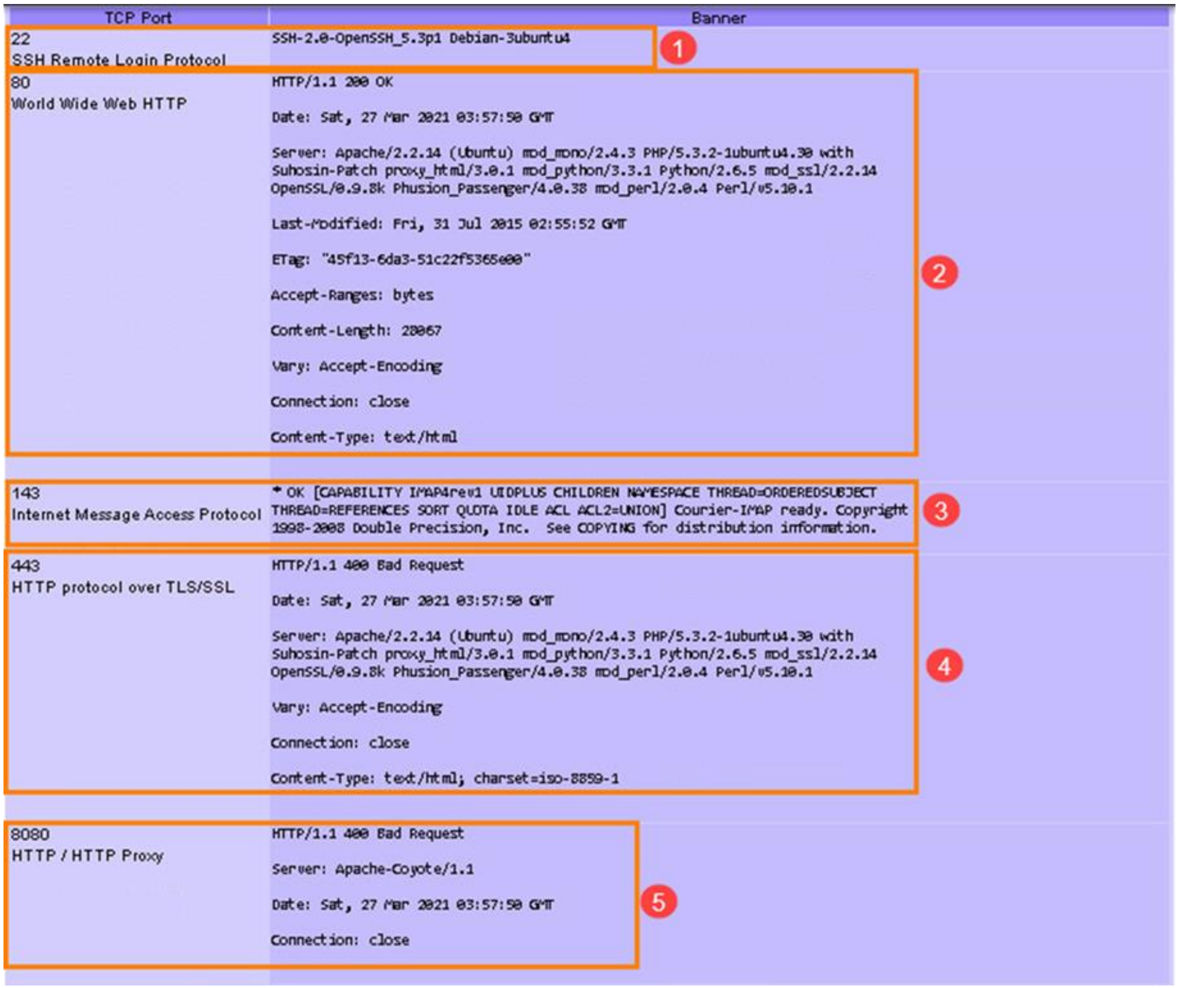
10. The report from the scan will open in the default web browser, and you will see the information displayed as seen below. In *item* **1,** the scan captured the NetBIOS name *OWASPBWA* and indicates that it is part of a workgroup and not a domain. In *item* **2,** you can see the details about the open TCP ports and the services they are running. *Item* **3** lists the open UDP ports and the services they are running. As you can see, UDP port 137 is running the NetBIOS service, which is where *SuperScan* got the NetBIOS name.



SuperScan Report - 03/26/21 20:57:42

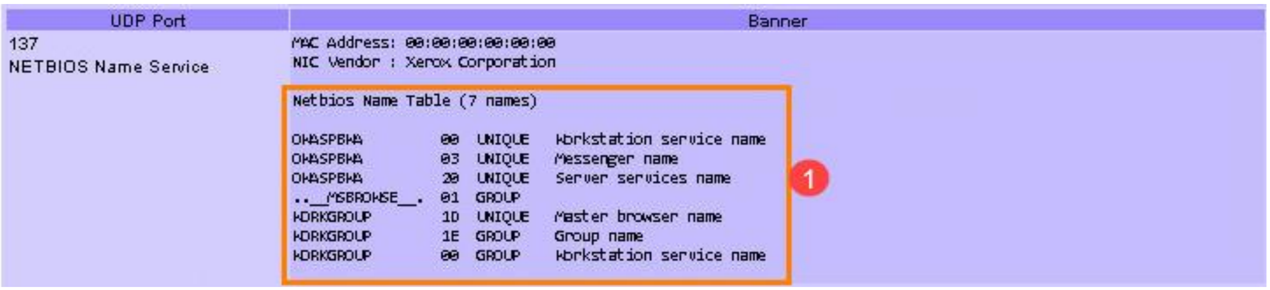
IP	192.168.68.12
Hostname	[Unknown]
Netbios Name	OWASPBWA
Workgroup/Domain	WORKGROUP
TCP Ports (8)	
22	SSH Remote Login Protocol
80	World Wide Web HTTP
139	NETBIOS Session Service
143	Internet Message Access Protocol
443	HTTP protocol over TLS/SSL
445	Microsoft-DS
8080	HTTP / HTTP Proxy
8081	HTTP / HTTP Proxy
UDP Ports (1)	
137	NETBIOS Name Service

11. The next section of the *SuperScan* report shows the banner grabbing attempt for each of the ports mentioned above. In *item* **1** below, we can see that SSH port 22 is running Open SSH on Debian Ubuntu. *Item* **2** shows that port 80 is running Apache server on Ubuntu. It also lists a last modified date for the “web page” and provides details such as content length and type. *Item* **3** shows that port 443 is running Internet Message Access Protocol (IMAP) which is used for email. The service is *Courier-IMAP. Items* **4** and **5** show that Apache server is running on both port 443 and 8080 as well. Based on what the above banner information is showing, we can safely assume that the host is running Ubuntu and is a web and email server.



TCP Port	Banner
22 SSH Remote Login Protocol	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu4
80 World Wide Web HTTP	HTTP/1.1 200 OK Date: Sat, 27 Mar 2021 03:57:50 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 Last-Modified: Fri, 31 Jul 2015 02:55:52 GMT ETag: "45f13-6da3-51c22f5365e00" Accept-Ranges: bytes Content-Length: 28067 Vary: Accept-Encoding Connection: close Content-Type: text/html
143 Internet Message Access Protocol	* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION] Courier-IMAP ready. Copyright 1998-2008 Double Precision, Inc. See COPYING for distribution information.
443 HTTP protocol over TLS/SSL	HTTP/1.1 400 Bad Request Date: Sat, 27 Mar 2021 03:57:50 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 Vary: Accept-Encoding Connection: close Content-Type: text/html; charset=iso-8859-1
8080 HTTP / HTTP Proxy	HTTP/1.1 400 Bad Request Server: Apache-Coyote/1.1 Date: Sat, 27 Mar 2021 03:57:50 GMT Connection: close

12. The banner information for the UDP port reveals the *NetBIOS Name Table* as seen in *item* **1.** It shows the NetBIOS names, workgroup, and domain names.



UDP Port	Banner
137 NETBIOS Name Service	MAC Address: 00:00:00:00:00:00 NIC Vendor : Xerox Corporation

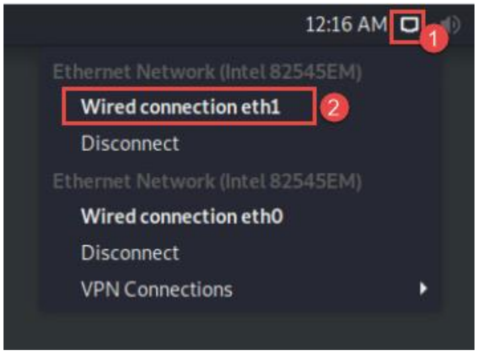
```
Netbios Name Table (7 names)

OWASPBWA        00  UNIQUE   Workstation service name
OWASPBWA        03  UNIQUE   Messenger name
OWASPBWA        20  UNIQUE   Server services name
..__MSBROWSE__. 01  GROUP
WORKGROUP       1D  UNIQUE   Master browser name
WORKGROUP       1E  GROUP    Group name
WORKGROUP       00  GROUP    Workstation service name
```

13. In this exercise, we enumerated NetBIOS names and grabbed banners. In the next exercise, we will perform LDAP enumeration and scan some more interesting data.

3 LDAP Enumeration

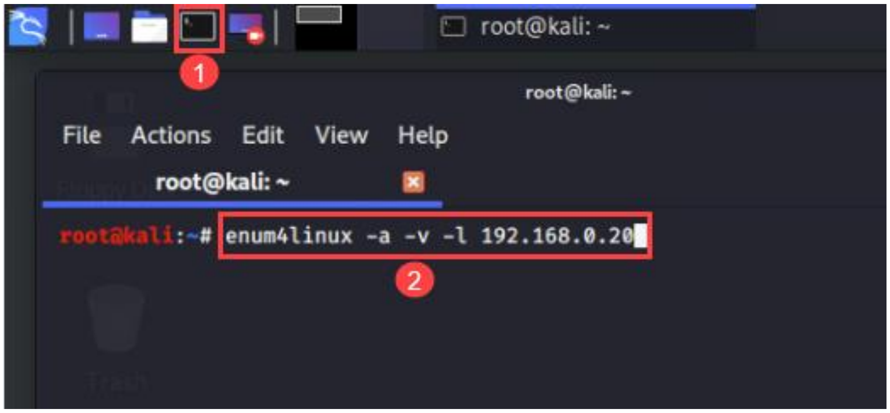
Enumerating active directory information is a great way to identify high-priority targets. As such, LDAP enumeration is vital when trying to move laterally to the most valuable host. In this exercise, we will perform LDAP enumeration of the Domain Controller.

1. Switch back to the Kali Linux VM. Before starting this task, ensure that the host machine is on the same network as the target machine. Select the **Ethernet network connection** from the navigation panel, as seen in *item* **1**. Then Click **Wired connection eth1** to allow *Kali Linux* to use the interface with the IP address 192.168.0.2, as seen in *item* **2**.



2. Let us begin by clicking the **Terminal** icon on the navigator panel, as seen in *item* **1.** Once the terminal window appears, type `enum4linux -a -v -l 192.168.0.20` and press **Enter** as seen in *item* **2.**

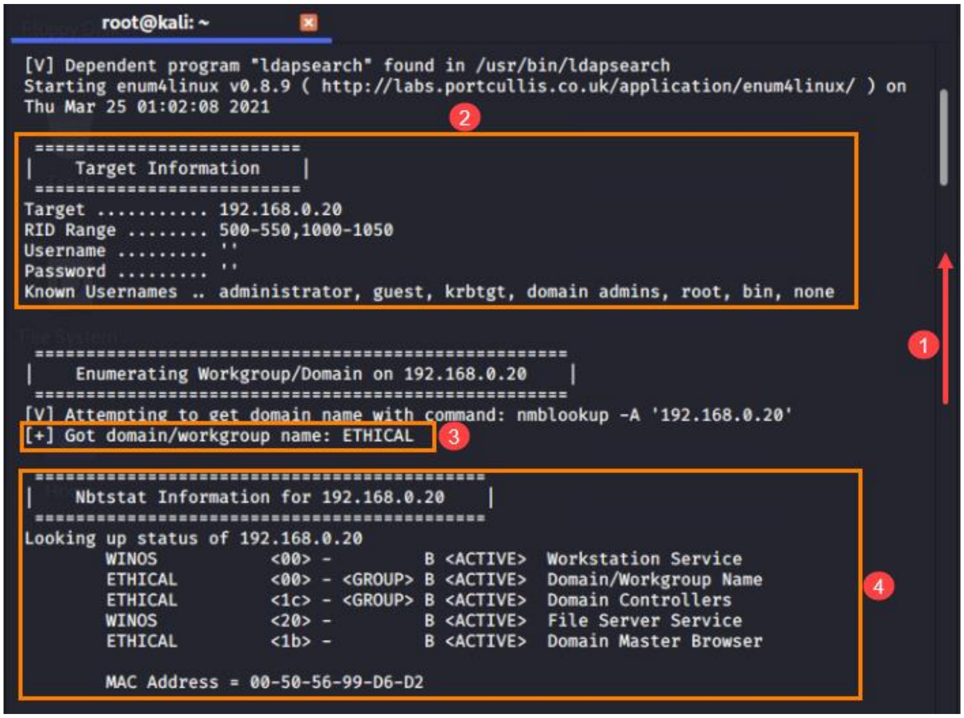
```
root@kali:~# enum4linux -a -v -l 192.168.0.20
```



```
root@kali:~# enum4linux -a -v -l 192.168.0.20
```

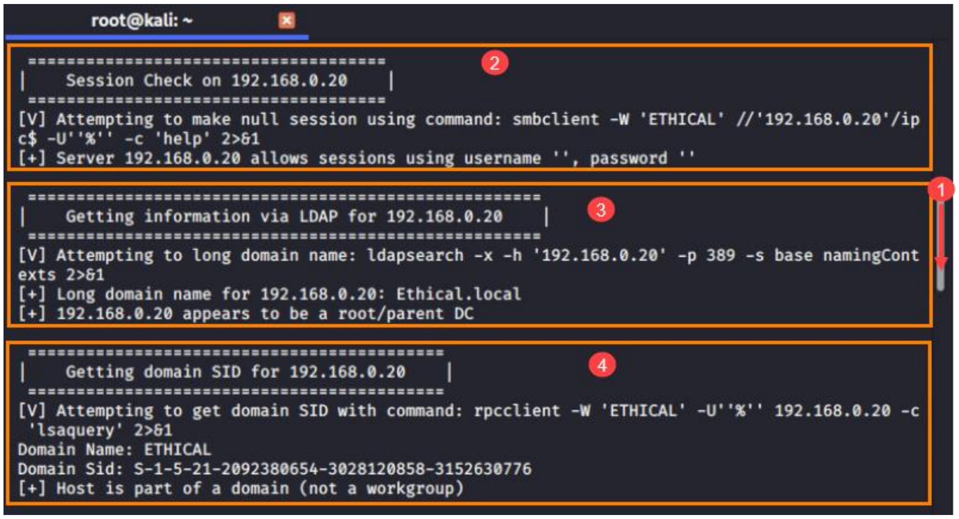
The *-a* switch instructs enum4linux to do a simple enumeration by grabbing userlist, sharelist, group and member list, password policy, RID cycle, OS information, nmb and printer information. The -v switch is verbose mode and the *-l* grabs ldap information. a stealthy SYN scan with version detection along with OS detection. Version detection collects information about the specific service running on an open port, including the product name and version

3. The results will populate the *Terminal* window. Let us scroll to the top using the mouse wheel or the scroll bar on the right, as seen in *item* **1.** The data highlighted in *item* **2** list the information being targeted. The next section highlighted in *item* **3** lists the known domain or workgroup. As you can see, the domain's name is *ETHICAL*. The *Nbtstat* information listed in the next section lists the NetBIOS name for the host, the domain group, and the MAC address, as seen in *item* **4.** As you can see, the host is in the *Domain Controllers* group, which indicates that it is a Domain Controller.



```
[V] Dependent program "ldapsearch" found in /usr/bin/ldapsearch
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on
Thu Mar 25 01:02:08 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.0.20
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on 192.168.0.20    |
 ====================================================
[V] Attempting to get domain name with command: nmblookup -A '192.168.0.20'
[+] Got domain/workgroup name: ETHICAL

 ============================================
|    Nbtstat Information for 192.168.0.20    |
 ============================================
Looking up status of 192.168.0.20
        WINOS           <00> -         B <ACTIVE>  Workstation Service
        ETHICAL         <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        ETHICAL         <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        WINOS           <20> -         B <ACTIVE>  File Server Service
        ETHICAL         <1b> -         B <ACTIVE>  Domain Master Browser

        MAC Address = 00-50-56-99-D6-D2
```

4. Let us scroll down a bit, as seen in *item* **1.** The next heading is *Session Check* which checks if a null session is possible. As you are already aware from the previous exercise, the null session is possible, as seen in *item* **2**. Below that, is the *LDAP* information seen in *item* **3.** This indicates that the long name for the host is *Ethical.local*. It also indicates that the host appears to be a *root/parent DC*. This is a great sign as it means it will have tons of information and can provide access to other accounts and devices. The heading below that is the *Security Identifier (SID),* as seen in *item* **4.** This SID uniquely identifies the domain.



```
 =====================================
|    Session Check on 192.168.0.20    |
 =====================================
[V] Attempting to make null session using command: smbclient -W 'ETHICAL' //'192.168.0.20'/ip
c$ -U''%'' -c 'help' 2>&1
[+] Server 192.168.0.20 allows sessions using username '', password ''

 =====================================================
|    Getting information via LDAP for 192.168.0.20    |
 =====================================================
[V] Attempting to long domain name: ldapsearch -x -h '192.168.0.20' -p 389 -s base namingCont
exts 2>&1
[+] Long domain name for 192.168.0.20: Ethical.local
[+] 192.168.0.20 appears to be a root/parent DC

 ===========================================
|    Getting domain SID for 192.168.0.20    |
 ===========================================
[V] Attempting to get domain SID with command: rpcclient -W 'ETHICAL' -U''%'' 192.168.0.20 -c
 'lsaquery' 2>&1
Domain Name: ETHICAL
Domain Sid: S-1-5-21-2092380654-3028120858-3152630776
[+] Host is part of a domain (not a workgroup)
```

5. The rest of the report did not show any results due to varying reasons; however, you can still scroll through it to see the commands that were used. It is important to note that these commands may provide more information if ran against more vulnerable systems.
6. This is the end of the lab; please close all windows and terminals to complete the lab.