

Creating an IT Asset Inventory (3e)

Managing Risk in Information Systems, Third Edition - Lab 05

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

14 hours, 39 minutes

Progress:

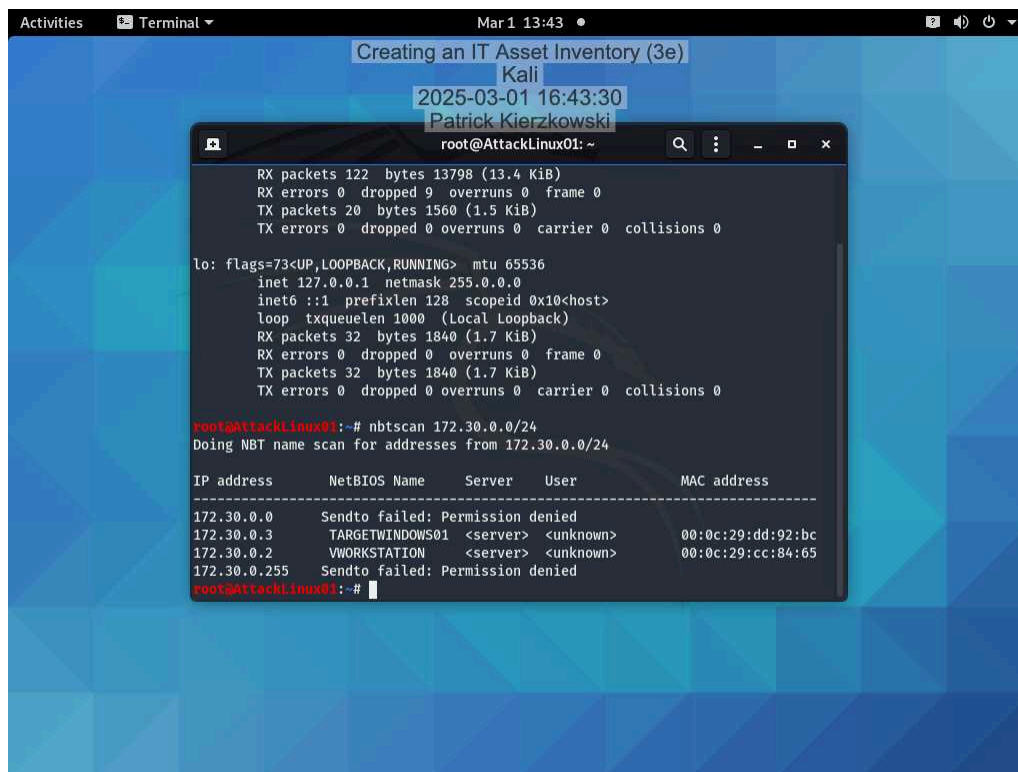
100%

Report Generated: Monday, July 7, 2025 at 9:39 PM

Guided Exercises

Part 1: Use Nbtscan and Nmap to Discover Computers

7. Make a screen capture showing the **nbtscan** results.



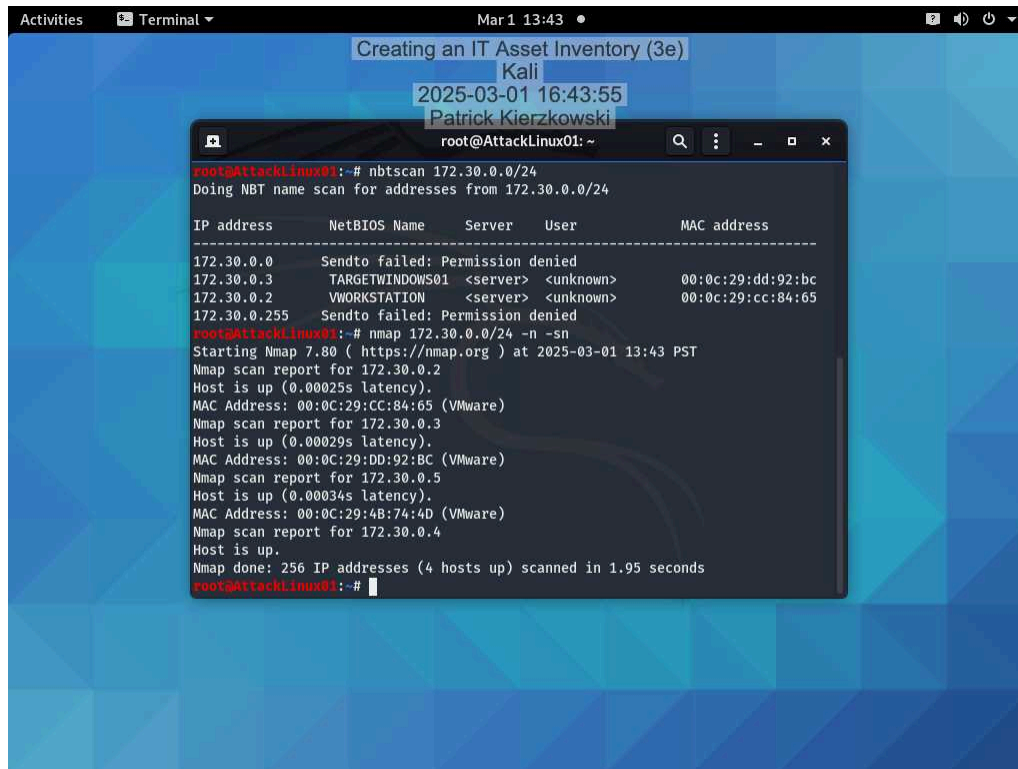
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@AttackLinux01: ~". The terminal output shows the results of an nbtscan command. The output includes network statistics for the interface 'lo' and the results of an NBT name scan for addresses from 172.30.0.0/24. The scan results are displayed in a table format with columns for IP address, NetBIOS Name, Server, User, and MAC address. The scan shows three results: 172.30.0.0 (Sendto failed: Permission denied), 172.30.0.3 (TARGETWINDOWS01 <server> <unknown>), and 172.30.0.2 (VWORKSTATION <server> <unknown>). The scan also shows a 'Sendto failed: Permission denied' error for 172.30.0.255.

```
root@AttackLinux01: ~  
RX packets 122 bytes 13798 (13.4 KiB)  
RX errors 0 dropped 9 overruns 0 frame 0  
TX packets 20 bytes 1560 (1.5 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 32 bytes 1840 (1.7 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 32 bytes 1840 (1.7 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@AttackLinux01:~# nbtscan 172.30.0.0/24  
Doing NBT name scan for addresses from 172.30.0.0/24  


| IP address   | NetBIOS Name                     | Server   | User      | MAC address       |
|--------------|----------------------------------|----------|-----------|-------------------|
| 172.30.0.0   | Sendto failed: Permission denied |          |           |                   |
| 172.30.0.3   | TARGETWINDOWS01                  | <server> | <unknown> | 00:0c:29:dd:92:bc |
| 172.30.0.2   | VWORKSTATION                     | <server> | <unknown> | 00:0c:29:cc:84:65 |
| 172.30.0.255 | Sendto failed: Permission denied |          |           |                   |

  
root@AttackLinux01:~#
```

9. Make a screen capture showing the Nmap results.



The screenshot shows a Kali Linux terminal window with the following content:

```
root@AttackLinux01: ~  
root@AttackLinux01:~# nbtscan 172.30.0.0/24  
Doing NBT name scan for addresses from 172.30.0.0/24  


| IP address   | NetBIOS Name                     | Server   | User      | MAC address       |
|--------------|----------------------------------|----------|-----------|-------------------|
| 172.30.0.0   | Sendto failed: Permission denied |          |           |                   |
| 172.30.0.3   | TARGETWINDOWS01                  | <server> | <unknown> | 00:0c:29:dd:92:bc |
| 172.30.0.2   | VWORKSTATION                     | <server> | <unknown> | 00:0c:29:cc:84:65 |
| 172.30.0.255 | Sendto failed: Permission denied |          |           |                   |

  
root@AttackLinux01:~# nmap 172.30.0.0/24 -n -sn  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-01 13:43 PST  
Nmap scan report for 172.30.0.2  
Host is up (0.00025s latency).  
MAC Address: 00:0C:29:CC:84:65 (VMware)  
Nmap scan report for 172.30.0.3  
Host is up (0.00029s latency).  
MAC Address: 00:0C:29:DD:92:BC (VMware)  
Nmap scan report for 172.30.0.5  
Host is up (0.00034s latency).  
MAC Address: 00:0C:29:4B:74:4D (VMware)  
Nmap scan report for 172.30.0.4  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.95 seconds  
root@AttackLinux01:~#
```

11. Record the OS Details or top five aggressive guesses for each host.

172.30.0.2 Top five aggressive guesses: Microsoft Windows Server 2012 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%).

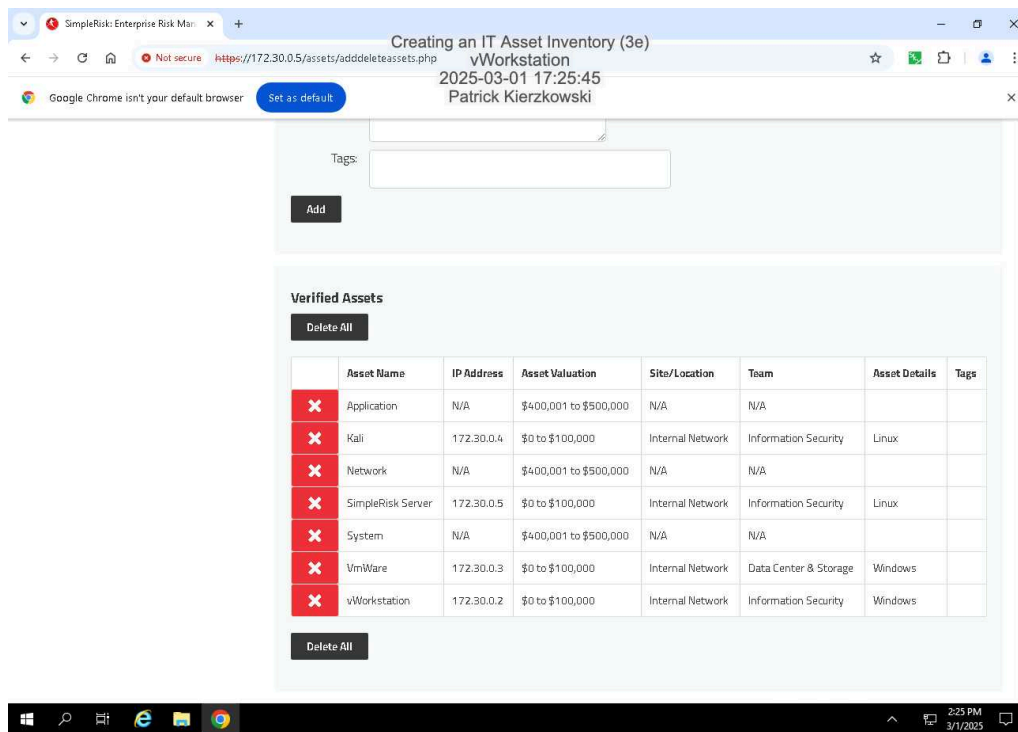
172.30.0.3. OS Details: Microsoft Windows Server 2016 build 10586 - 14393. 172.30.0.5 Top five aggressive guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 -3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%). 172.30.0.4. OS Details: Linux 2.6.32

Part 2: Use SimpleRisk to Document IT Assets

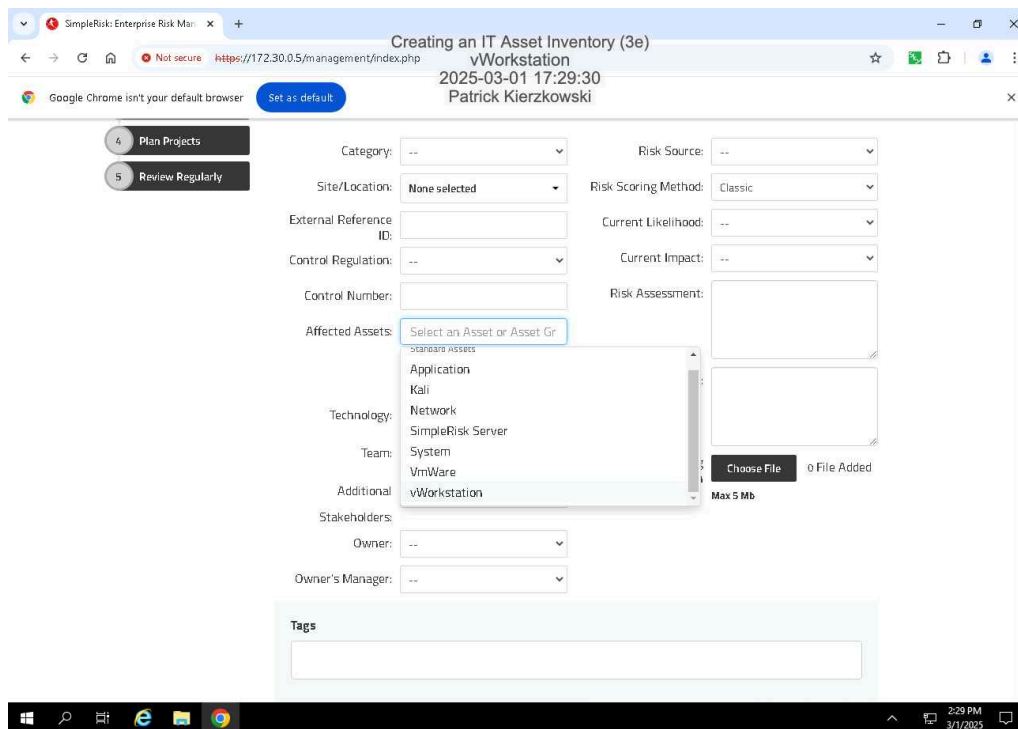
Creating an IT Asset Inventory (3e)

Managing Risk in Information Systems, Third Edition - Lab 05

20. Make a screen capture showing the **updated Verified Assets list**.



23. Make a screen capture showing the **Affected Assets list**.

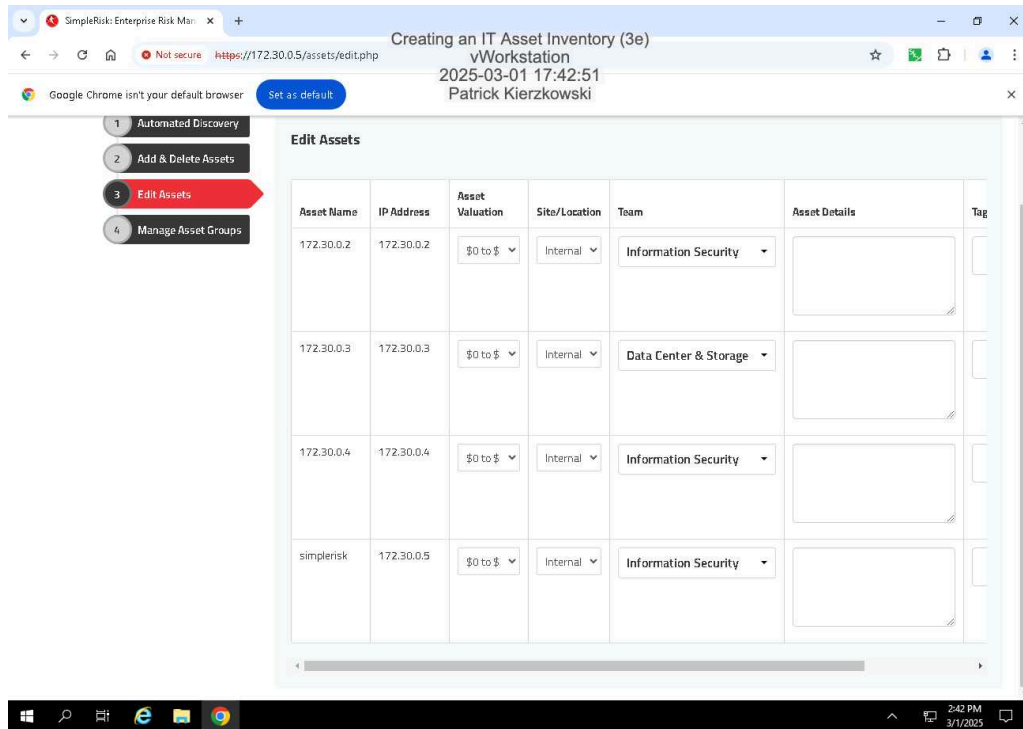


Part 3: Use SimpleRisk to Perform Automated Discovery

Creating an IT Asset Inventory (3e)

Managing Risk in Information Systems, Third Edition - Lab 05

8. Make a screen capture showing the updated Edit Assets page.



Challenge Exercise

Make a screen capture showing the **complete list of verified assets**.

