

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:

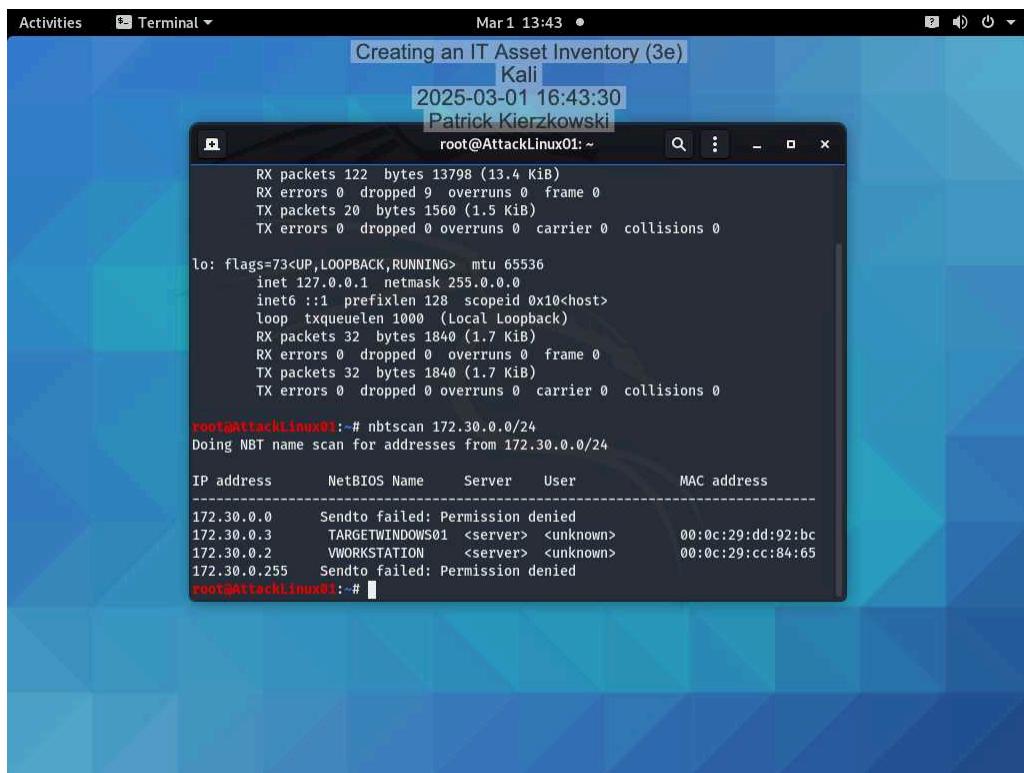
100%

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.



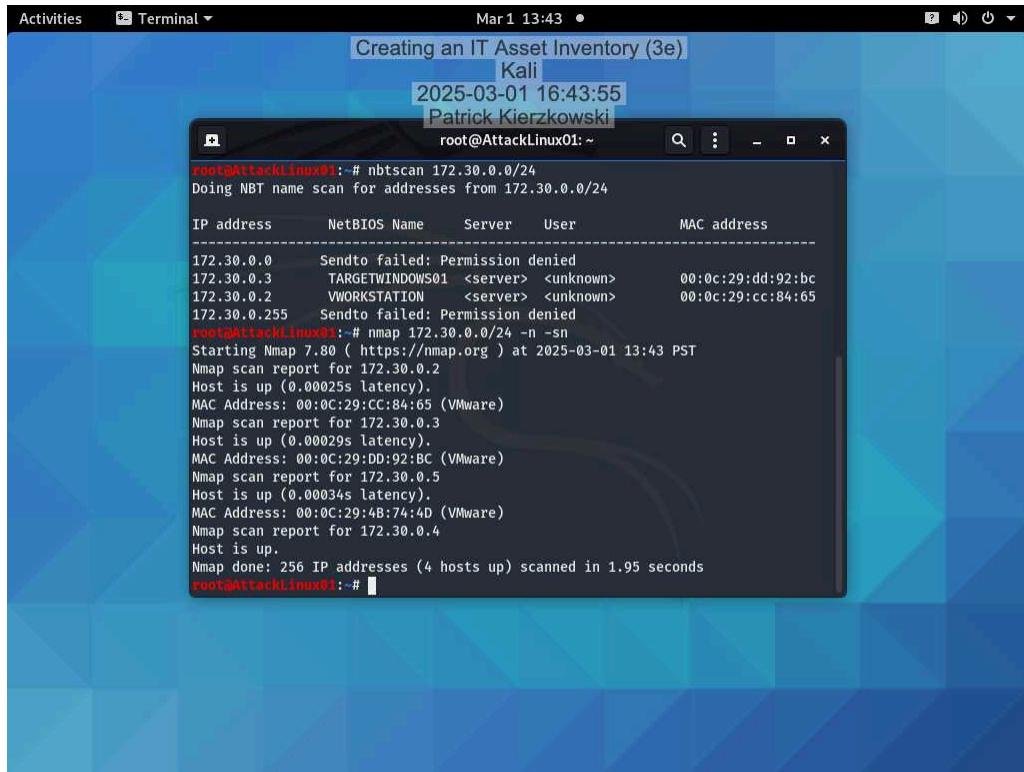
The screenshot shows a terminal window titled "root@AttackLinux01: ~" running on a Kali Linux desktop environment. The terminal displays the output of the nbtscan command. It starts with network statistics for the lo interface, followed by the nbtscan command itself, which scans for NBT names on the 172.30.0.0/24 subnet. The results table lists four entries, all of which failed due to permission denied.

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			

Creating an IT Asset Inventory (3e)

Managing Risk in Information Systems, Third Edition - Lab 05

9. Make a screen capture showing the Nmap results.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title bar reads "Creating an IT Asset Inventory (3e) Kali". The terminal content displays two command-line sessions:

```
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:D0:92: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.

The screenshot shows a web browser window titled "Creating an IT Asset Inventory (3e)". The URL is <https://172.30.0.5/assets/adddelteassets.php>. The page displays a table of "Verified Assets" with the following data:

	Asset Name	IP Address	Asset Valuation	Site/Location	Team	Asset Details	Tags
X	Application	N/A	\$400,001 to \$500,000	N/A	N/A		
X	Kali	172.30.0.4	\$0 to \$100,000	Internal Network	Information Security	Linux	
X	Network	N/A	\$400,001 to \$500,000	N/A	N/A		
X	SimpleRisk Server	172.30.0.5	\$0 to \$100,000	Internal Network	Information Security	Linux	
X	System	N/A	\$400,001 to \$500,000	N/A	N/A		
X	VmWare	172.30.0.3	\$0 to \$100,000	Internal Network	Data Center & Storage	Windows	
X	vWorkstation	172.30.0.2	\$0 to \$100,000	Internal Network	Information Security	Windows	

At the top of the table, there is a "Delete All" button. At the bottom, there is another "Delete All" button. The browser status bar at the bottom right shows "2:25 PM 3/1/2025".

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

The screenshot shows a web browser window titled "Creating an IT Asset Inventory (3e)". The URL is <https://172.30.0.5/management/index.php>. The page displays a form for managing assets, with a dropdown menu open under the "Affected Assets" field. The menu lists several assets:

- standard assets
- Application
- Kali
- Network
- SimpleRisk Server
- System
- VmWare
- vWorkstation

The "Affected Assets" field has a placeholder "Select an Asset or Asset Gr". To the right of the dropdown, there is a "Choose File" button with "0 File Added" and "Max 5 Mb" text. The browser status bar at the bottom right shows "2:29 PM 3/1/2025".

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.

The screenshot shows a web browser window titled "Creating an IT Asset Inventory (3e)" with the URL <https://172.30.0.5/assets/edit.php>. The page displays a table of assets with the following data:

Asset Name	IP Address	Asset Valuation	Site/Location	Team	Asset Details	Tag
172.30.0.2	172.30.0.2	\$0 to \$	Internal	Information Security		
172.30.0.3	172.30.0.3	\$0 to \$	Internal	Data Center & Storage		
172.30.0.4	172.30.0.4	\$0 to \$	Internal	Information Security		
simplerisk	172.30.0.5	\$0 to \$	Internal	Information Security		

The left sidebar has four buttons: 1. Automated Discovery, 2. Add & Delete Assets, 3. Edit Assets (highlighted with a red arrow), and 4. Manage Asset Groups. The top right shows the date and time: 2025-03-01 17:42:51 and the user: Patrick Kierzkowski. The bottom status bar shows the date and time: 2:42 PM 3/1/2025.

Creating an IT Asset Inventory (3e)

Managing Risk in Information Systems, Third Edition - Lab 05

Challenge Exercise

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

The screenshot shows a web browser window with the following details:

- Title Bar:** SimpleRisk: Enterprise Risk Man... (partially visible), Not secure, https://172.30.0.5/assets/adddelteassets.php, 2025-03-01 18:31:18, Patrick Kierzkowski.
- Form (Top):** A form for adding a new asset. It includes fields for 'Asset Name' (vWorkstation), 'IP Address' (192.168.1.2), 'Asset Valuation' (\$10,001 to \$50,000), 'Site/Location' (Server Room), 'Team' (Data Center & Storage), 'Asset Details' (Windows Server 2016), and 'Tags'. A green success message 'Asset was added successfully.' is displayed.
- Table (Bottom):** A table titled 'Verified Assets' showing the following data:

	Asset Name	IP Address	Asset Valuation	Site/Location	Team	Asset Details	Tags
X	File server	192.168.1.2	\$10,001 to \$50,000	Server Room	Data Center & Storage	Windows Server 2016	
X	Layer 3 switch	192.168.1.231	\$0 to \$10,000	Server Room	Network	Cisco IOS	
X	Teleconference device	192.168.1.230	\$0 to \$10,000	Conference room	Collaboration	Embedded linux	
X	Used computer 1	192.168.1.20	\$0 to \$10,000	Office Area	Business Unit	Windows 10	
X	Used computer 2	192.168.1.21	\$0 to \$10,000	Office Area	Business Unit	Windows 10	