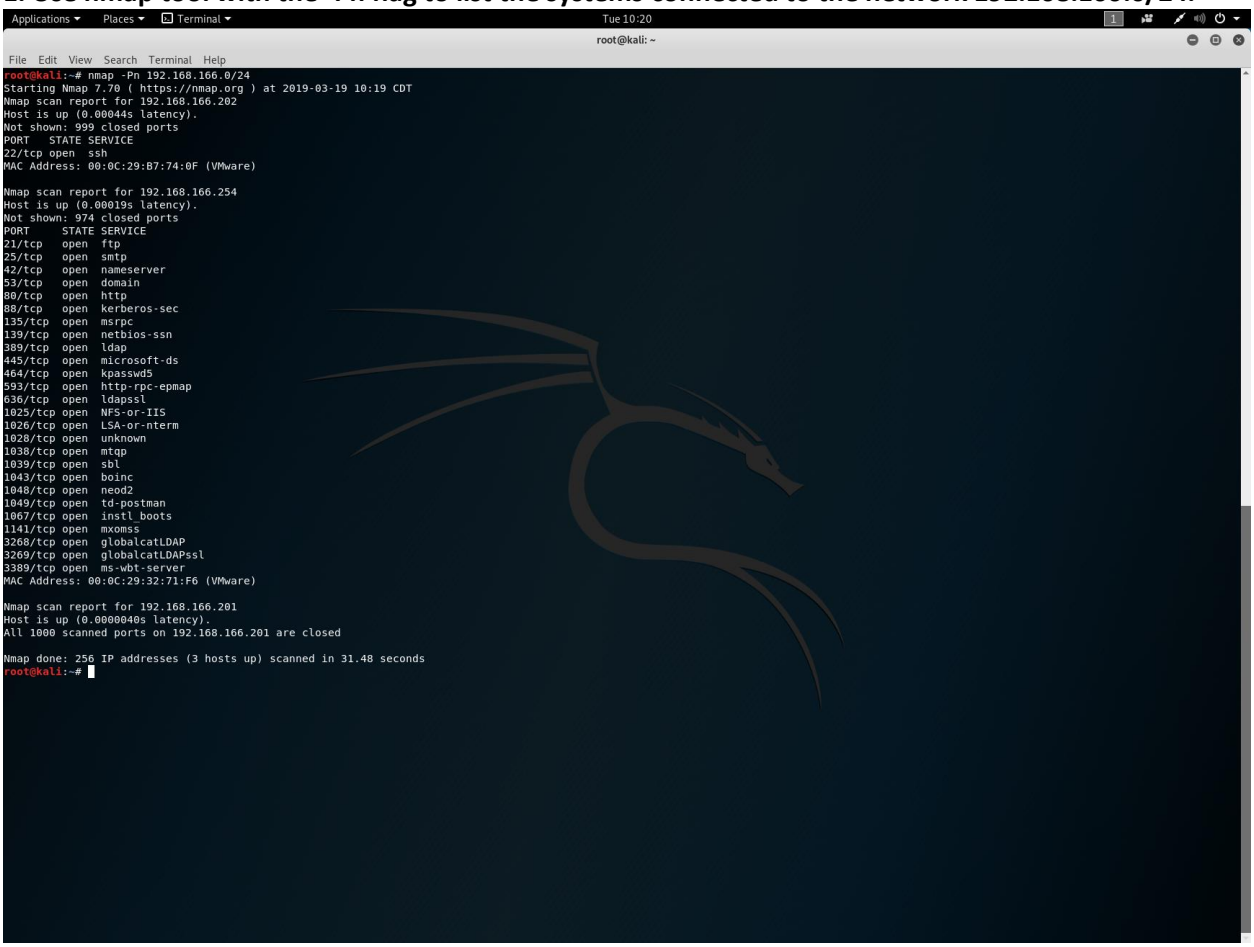
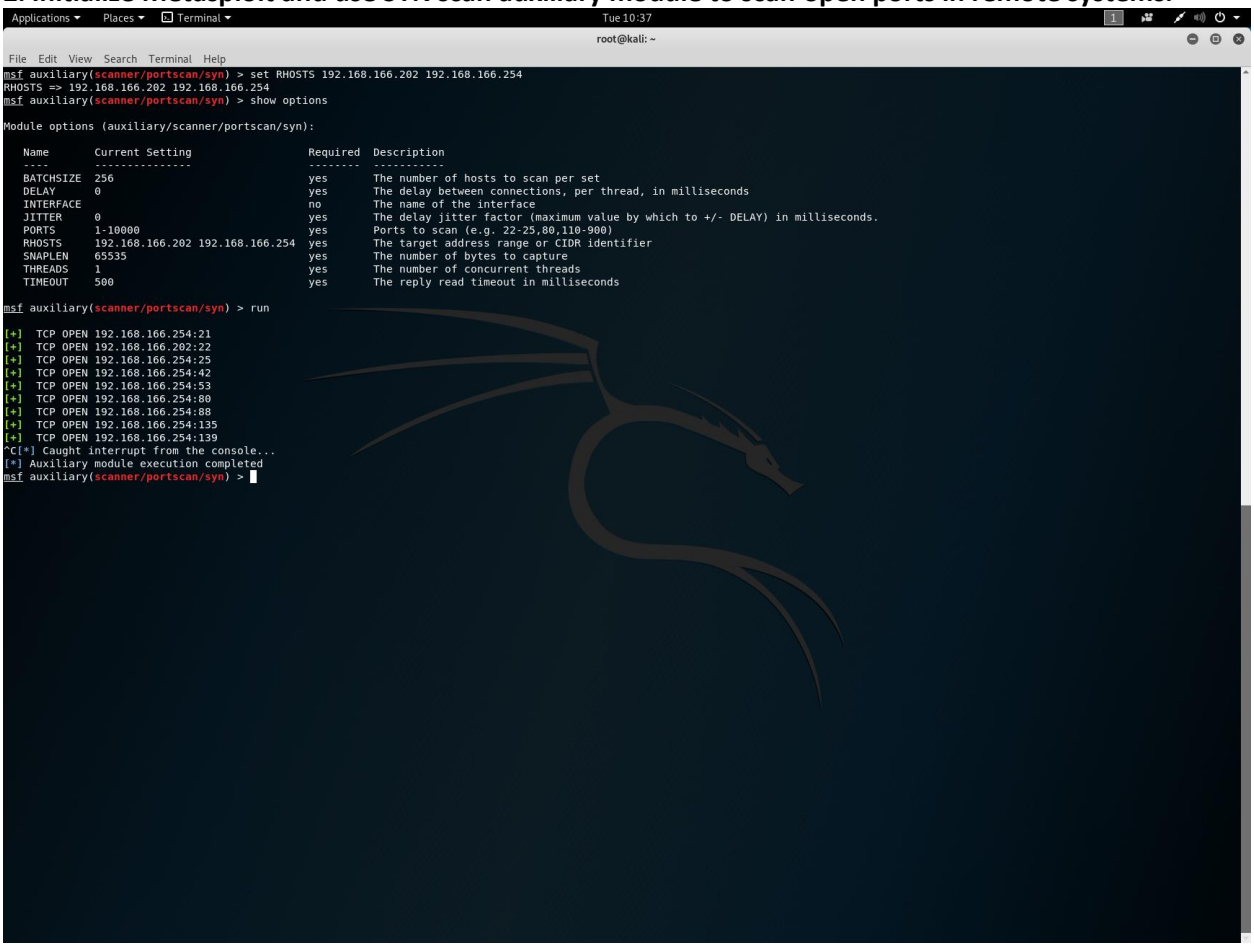
1. Use nmap tool with the -Pn flag to list the systems connected to the network 192.168.166.0/24.



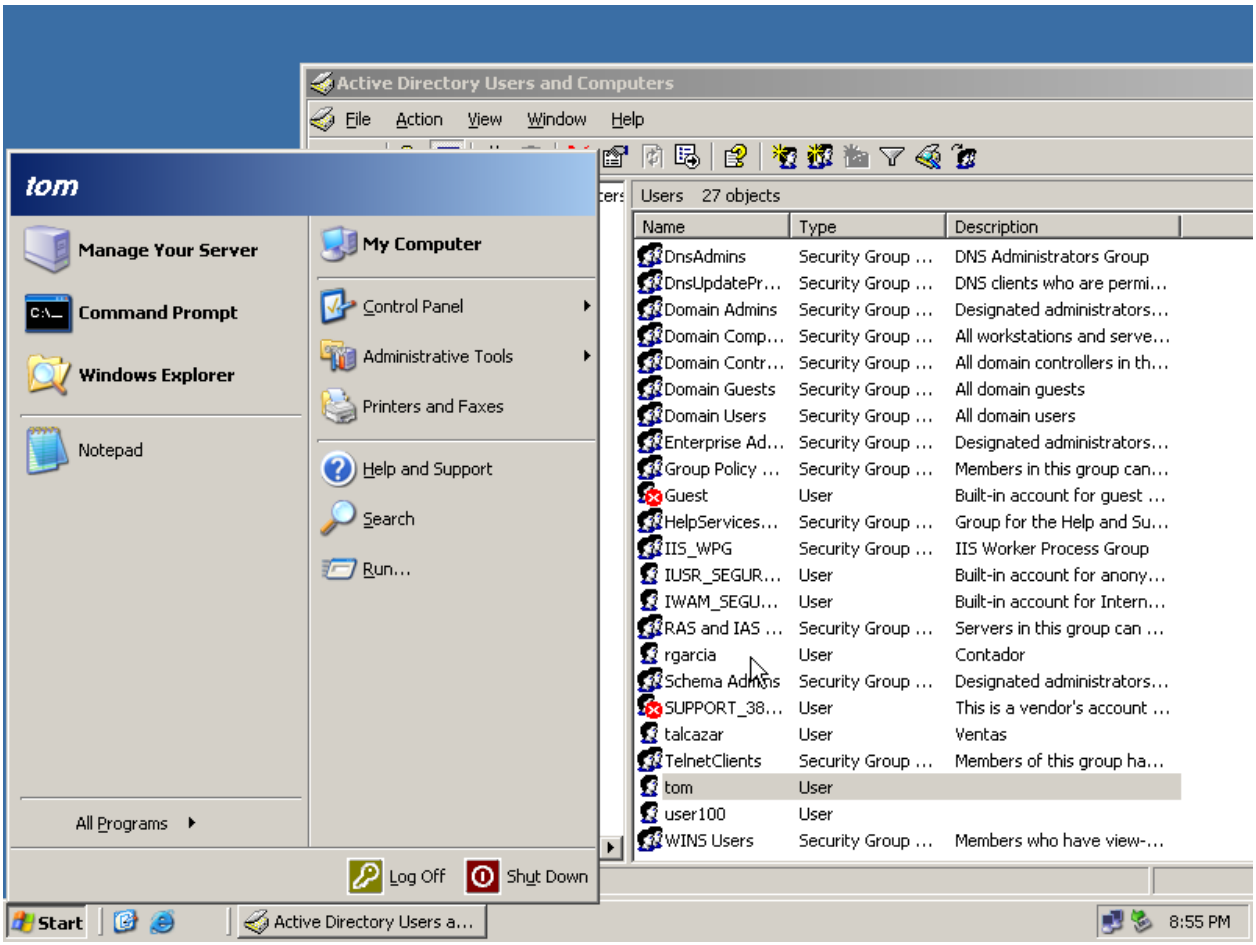
2. Initialize Metasploit and use SYN scan auxiliary module to scan open ports in remote systems.

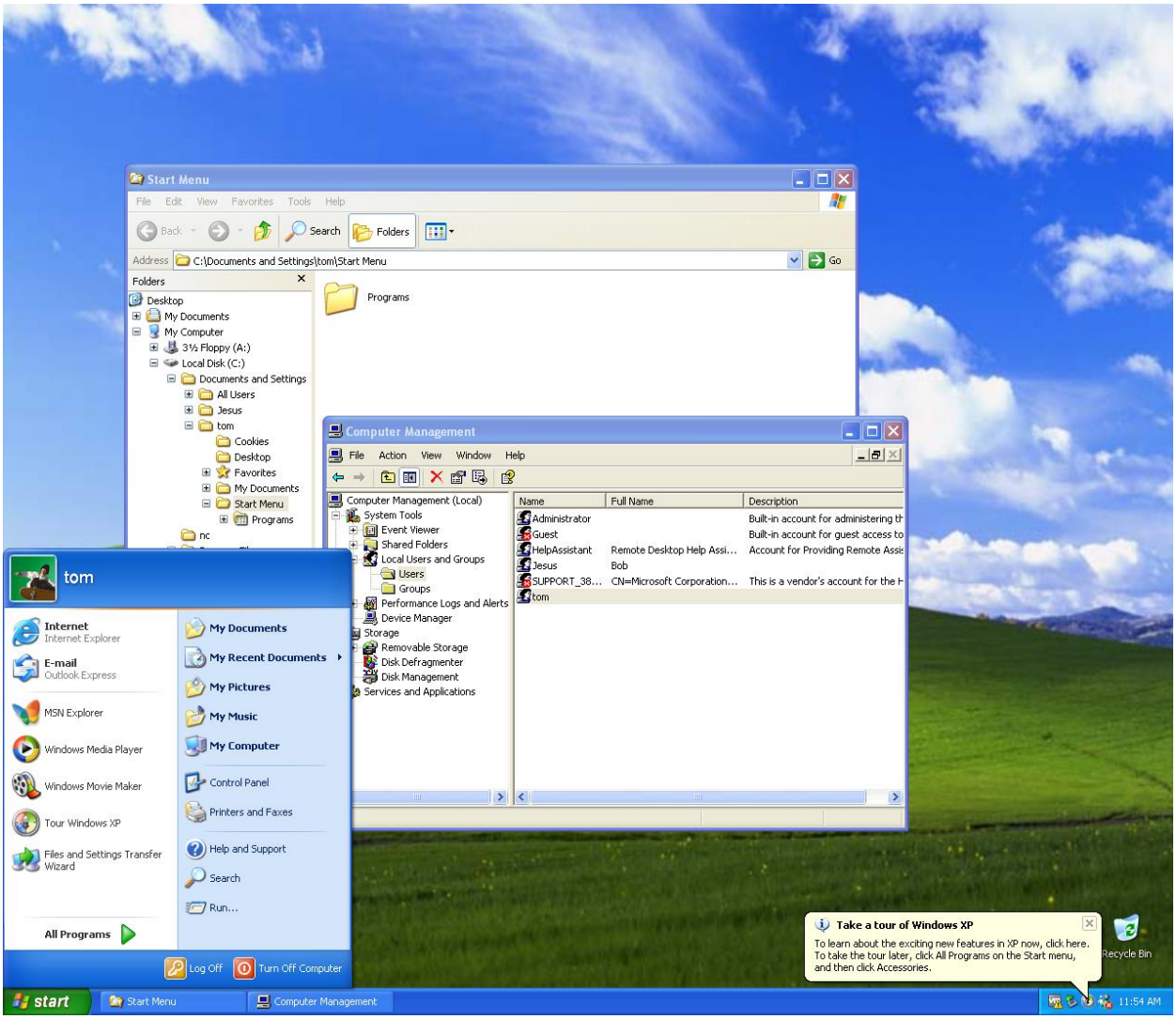


3. Describe the benefit(s) of using SYN scan vs TCP scan.

SYN scan drops the connection once port information is received from the target. If a SYN/ACK packet is received then the target port is listening, and if a RST/ACK packet is received then the port is not listening. On the other hand, TCP scan does not need administrative privileges on the source machine but is more susceptible to be detected by network monitoring systems due to the 3-way connection handshake.

4. Using the mc03_026_dcom Exploit and the windows/adduser Payload create the tom user and a password for TWXP0 and TW3P0 VMs


Active Directory Users and Computers
File Action View Window Help
tom
Manage Your Server
Command Prompt
Windows Explorer
Notepad
My Computer
Control Panel
Administrative Tools
Printers and Faxes
Help and Support
Search
Run...
All Programs
Log Off
Shut Down
Users 27 objects
Name Type Description
DnsAdmins Security Group ... DNS Administrators Group
DnsUpdatePr... Security Group ... DNS clients who are permi...
Domain Admins Security Group ... Designated administrators...
Domain Comp... Security Group ... All workstations and serve...
Domain Contr... Security Group ... All domain controllers in th...
Domain Guests Security Group ... All domain guests
Domain Users Security Group ... All domain users
Enterprise Ad... Security Group ... Designated administrators...
Group Policy ... Security Group ... Members in this group can...
Guest User Built-in account for guest ...
HelpServices... Security Group ... Group for the Help and Su...
IIS_WPG Security Group ... IIS Worker Process Group
IUSR_SEGUR... User Built-in account for anony...
IWAM_SEGU... User Built-in account for Intern...
RAS and IAS ... Security Group ... Servers in this group can ...
rgarcia User Contador
Schema Admins Security Group ... Designated administrators...
SUPPORT_38... User This is a vendor's account ...
talcazar User Ventas
TelnetClients Security Group ... Members of this group ha...
tom User
user100 User
WINS Users Security Group ... Members who have view-...
Start
Active Directory Users a...
8:55 PM


Start Menu
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\tom\Start Menu
Go
Folders
Desktop
My Documents
My Computer
3½ Floppy (A:)
Local Disk (C:)
Documents and Settings
All Users
Jesus
tom
Cookies
Desktop
Favorites
My Documents
Start Menu
Programs
nc
Programs
Computer Management
File Action View Window Help
Computer Management (Local)
System Tools
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance Logs and Alerts
Device Manager
Storage
Removable Storage
Disk Defragmenter
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering th
Guest
Built-in account for guest access to
HelpAssistant
Remote Desktop Help Assi...
Account for Providing Remote Assis
Jesus
Bob
SUPPORT_38...
CN=Microsoft Corporation...
This is a vendor's account for the H
tom
tom
Internet
Internet Explorer
E-mail
Outlook Express
MSN Explorer
Windows Media Player
Windows Movie Maker
Tour Windows XP
Files and Settings Transfer Wizard
All Programs
My Documents
My Recent Documents
My Pictures
My Music
My Computer
Control Panel
Printers and Faxes
Help and Support
Search
Run...
Log Off
Turn Off Computer
Take a tour of Windows XP
To learn about the exciting new features in XP now, click here. To take the tour later, click All Programs on the Start menu, and then click Accessories.
Recycle Bin
start
Start Menu
Computer Management
11:54 AM