Module 03: Information Security Threats and Vulnerability Assessment

Scenario

A threat is a potential occurrence of an undesirable event that can eventually damage and disrupt the operational and functional activities of an organization. Threat can be any type of entity or action performed on physical or intangible asset that can disrupt the security. The existence of threats may be accidental, intentional, or due to the impact of some other action. Attackers use cyber threats to infiltrate and steal data such as individual's personal information, financial information, and login credentials. They can also use the compromised system to perform malicious activities and launch further attacks. The criticality of a threat is based on how much damage it will cause, or how uncontrollable it is, or how complicated it is to identify the latest discovered threat incident in advance. Threats to data assets cause loss of confidentiality, integrity, or availability (CIA) of data. They also result in data loss, identity theft, cyber sabotage, and information disclosure.

The lab activities in this module provide first-hand experience with various techniques that attackers use to write and propagate malware. You will also learn how to effectively perform vulnerability assessment to determine security vulnerabilities in the target system or network.

Objective

The objective of the lab is to create malware and perform other tasks that include, but are not limited to:

- Create a Trojan and exploit a target machine
- Create a virus to infect the target machine
- Perform vulnerability assessment to identify security vulnerabilities in the target system or network

Overview of Threats

Following are various sources from which threats originate and can be broadly classified as natural threats, unintentional threats, and intentional threats.

- **Natural Threats**: Natural factors such as fires, floods, power failures, lightning, meteor, and earthquakes are potential threats to the assets of an organization. For example, these may cause severe physical damage to computer systems.
- **Unintentional Threats**: Unintentional threats are threats that exist due to the potential for unintentional errors occurring within the organization. Examples

include insider-originating security breaches, negligence, operator errors, unskilled administrators, lazy or untrained employees, and accidents.

- **Intentional Threats**: There are two sources of intentional threats.
- **Internal Threats**: Most computer and Internet-related crimes are insiders or internal attacks. These threats are performed by insiders within the organization such as disgruntled or negligent employees and harm the organization intentionally or unintentionally. Most of these attacks are performed by privileged users of the network.
- **External Threats**: External attacks are performed by exploiting vulnerabilities that already exist in the network, without the assistance of insider employees. Therefore, the potential to perform an external attack depends on the severity of the identified network weaknesses.

Lab Tasks

Ensure that the **Windows Defender Firewall is Turn off** on the machines you are using for the lab tasks in this module, as it blocks and deletes malware as soon as it is executed.

We can use numerous tools and techniques to gain access to the target network or machine. Recommended labs that will assist you in learning various malware attack and vulnerability assessment techniques include:

1. Create a Trojan to gain access to the target system
    - Create a Trojan server using Theef RAT trojan
    - Gain control over a victim machine using the njRAT RAT Trojan
2. Create a virus to infect the target system
    - Create a virus using the JPS Virus Maker Tool and infect the target system
3. Perform vulnerability assessment to identify security vulnerabilities in the target system or network
    - Perform vulnerability analysis using OpenVAS

Lab 1: Create a Trojan to Gain Access to the Target System

Lab Scenario

A Trojan is wrapped within or attached to a legitimate program, meaning that the program may have functionality that is not apparent to the user. Furthermore, attackers use victims

as unwitting intermediaries to attack others. They can use a victim's computer to commit illegal DoS attacks.

A compromised system can affect other systems on the network. Systems that transmit authentication credentials such as passwords over shared networks in clear text or a trivially encrypted form are particularly vulnerable. If an intruder compromises a system on such a network, he or she may be able to record usernames and passwords or other sensitive information.

Additionally, a Trojan, depending on the actions it performs, may falsely implicate a remote system as the source of an attack by spoofing, thereby causing the remote system to incur a liability. Trojans enter the system by means such as email attachments, downloads, and instant messages.

The lab tasks in this exercise demonstrate how easily hackers can gain access to the target systems in the organization and create a covert communication channel for transferring sensitive data between the victim computer and the attacker.

Lab Objectives

- Create a Trojan Server using Theef RAT Trojan
- Gain Control over a Victim Machine using the njRAT RAT Trojan

---

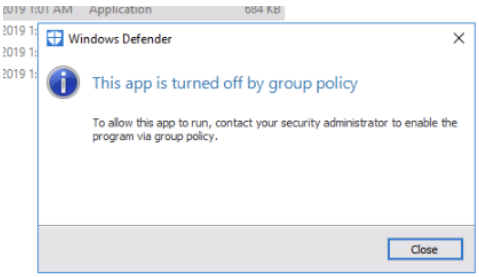
Task 1: Create a Trojan Server using Theef RAT Trojan

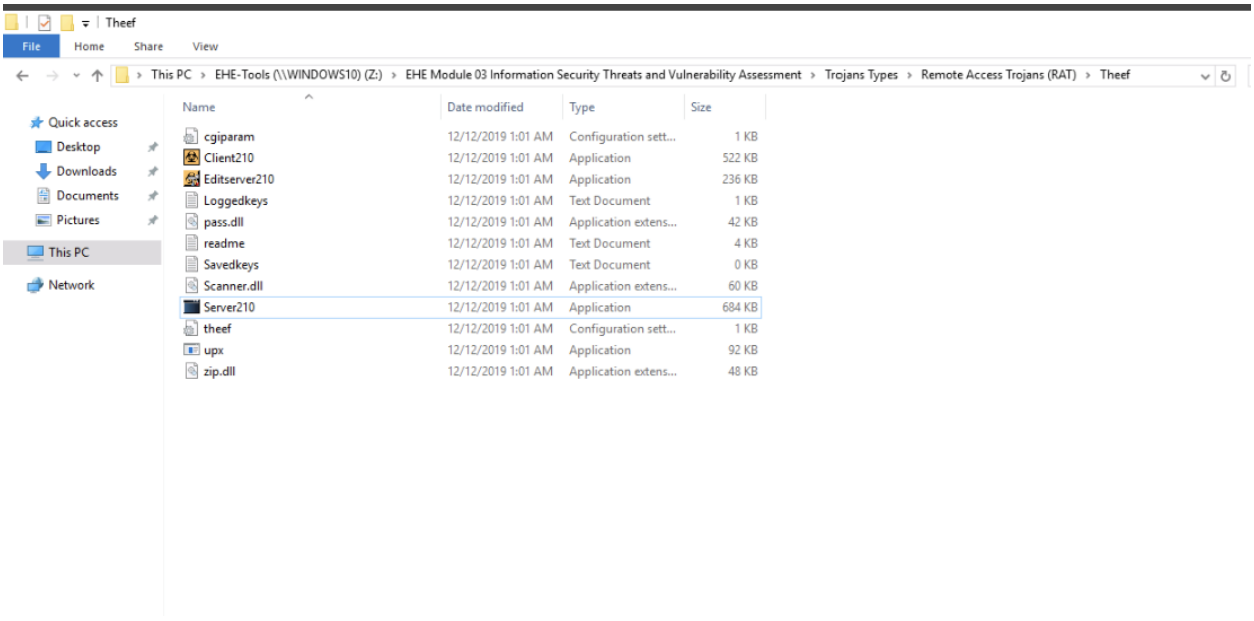
Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks. The virus infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

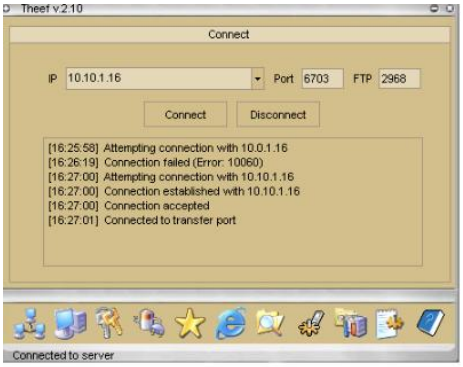
Theef is a Remote Access Trojan written in Delphi. It allows remote attackers access to the system via port 9871. Theef is a Windows-based application for both client and server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

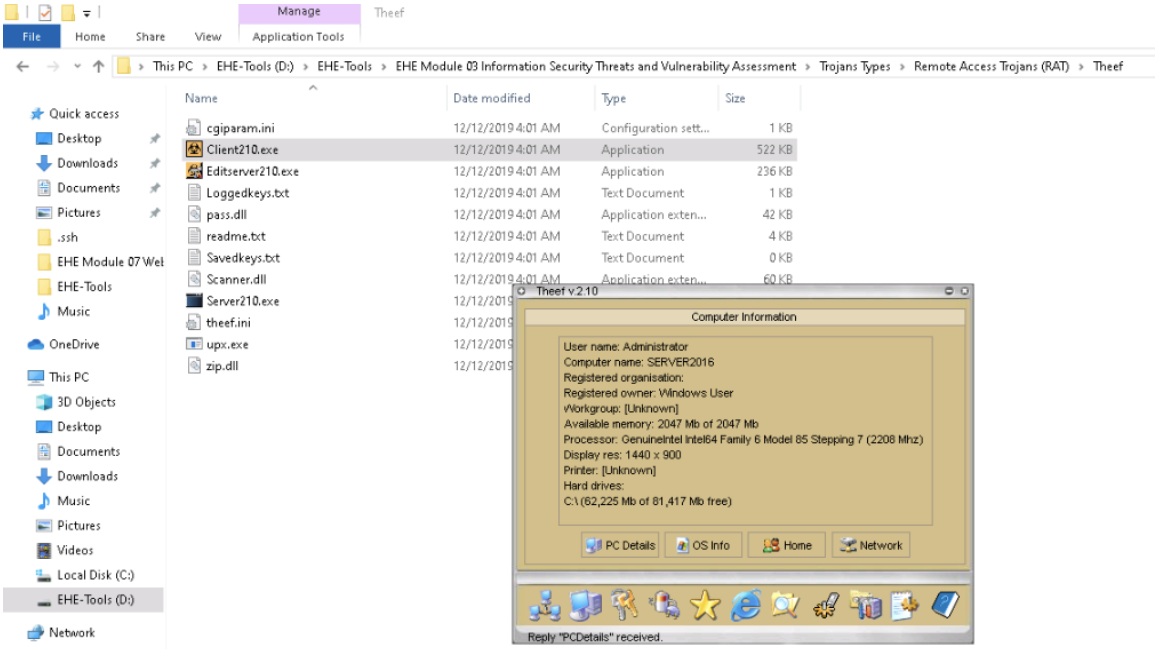
The versions of the created client or host, and the appearance of its website, may differ from that of this lab. However, the actual process of creating the server and the client is the same.

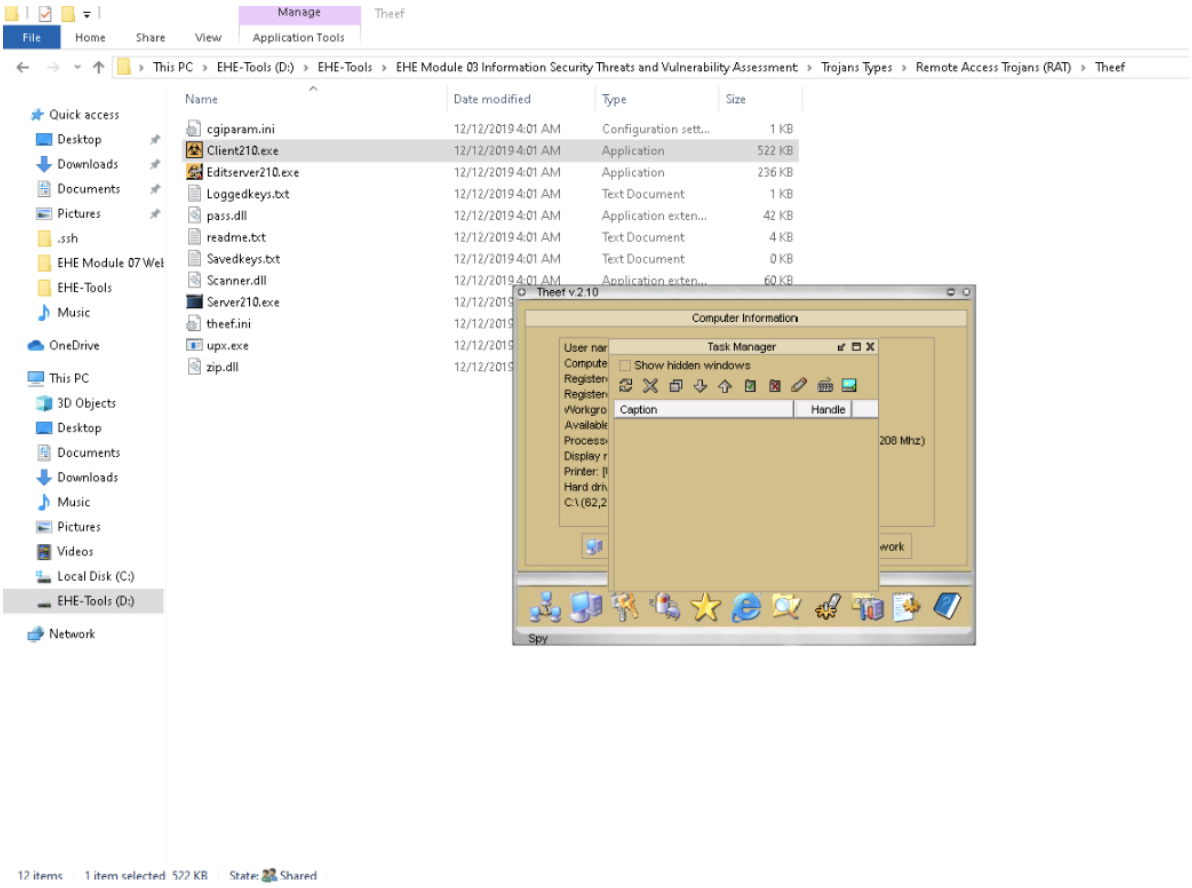
Generally, an attacker might send a server executable to the victim machine and entice the victim into running it. In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2016**.

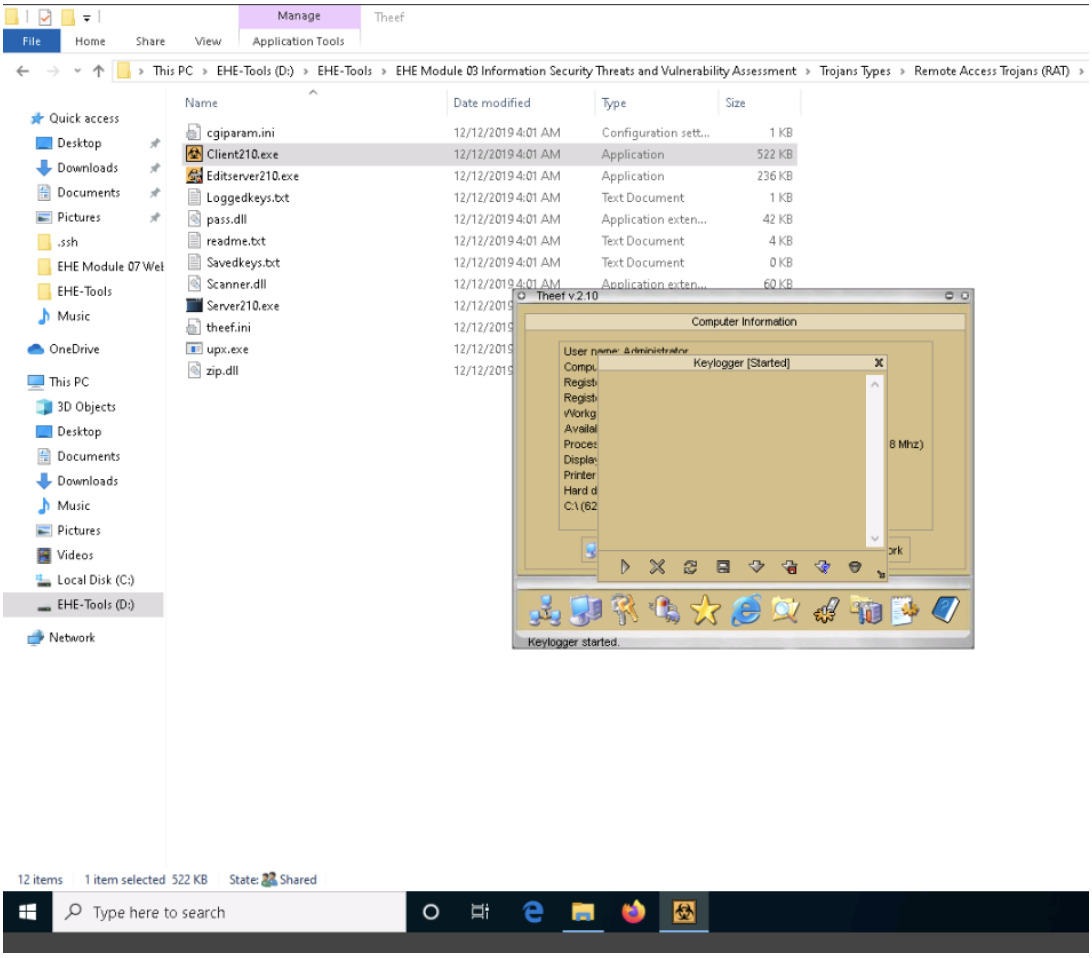


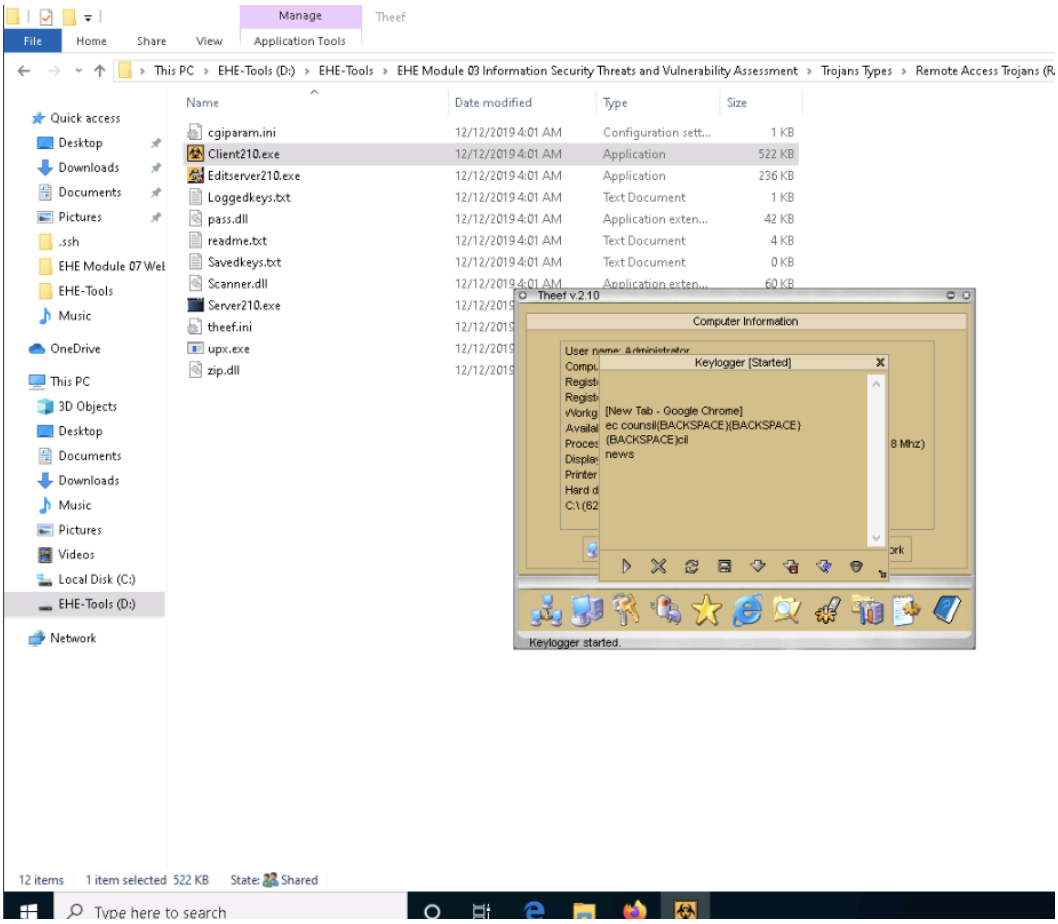



Theef v.2.10
Connect
IP 10.10.1.16
Port 6703
FTP 2968
Connect
Disconnect
[16:25:58] Attempting connection with 10.0.1.16
[16:26:19] Connection failed (Error: 10060)
[16:27:00] Attempting connection with 10.10.1.16
[16:27:00] Connection established with 10.10.1.16
[16:27:00] Connection accepted
[16:27:01] Connected to transfer port
Connected to server


Manage
Theef
File
Home
Share
View
Application Tools
This PC › EHE-Tools (D:) › EHE-Tools › EHE Module 03 Information Security Threats and Vulnerability Assessment › Trojans Types › Remote Access Trojans (RAT) › Theef
Quick access
Desktop
Downloads
Documents
Pictures
.ssh
EHE Module 07 Wel
EHE-Tools
Music
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
EHE-Tools (D:)
Network
Name
Date modified
Type
Size
cgiparam.ini 12/12/2019 4:01 AM Configuration sett... 1 KB
Client210.exe 12/12/2019 4:01 AM Application 522 KB
Editserver210.exe 12/12/2019 4:01 AM Application 236 KB
Loggedkeys.txt 12/12/2019 4:01 AM Text Document 1 KB
pass.dll 12/12/2019 4:01 AM Application exten... 42 KB
readme.txt 12/12/2019 4:01 AM Text Document 4 KB
Savedkeys.txt 12/12/2019 4:01 AM Text Document 0 KB
Scanner.dll 12/12/2019 4:01 AM Application exten... 60 KB
Server210.exe
theef.ini
upx.exe
zip.dll
Theef v.2.10
Computer Information
User name: Administrator
Computer name: SERVER2016
Registered organisation:
Registered owner: Windows User
Workgroup: [Unknown]
Available memory: 2047 Mb of 2047 Mb
Processor: GenuineIntel Intel64 Family 6 Model 85 Stepping 7 (2208 Mhz)
Display res: 1440 x 900
Printer: [Unknown]
Hard drives:
C:\ (62,225 Mb of 81,417 Mb free)
PC Details
OS Info
Home
Network
Reply "PCDetails" received.


Manage
Theef
File
Home
Share
View
Application Tools
This PC › EHE-Tools (D:) › EHE-Tools › EHE Module 03 Information Security Threats and Vulnerability Assessment › Trojans Types › Remote Access Trojans (RAT) › Theef
Quick access
Desktop
Downloads
Documents
Pictures
.ssh
EHE Module 07 Wel
EHE-Tools
Music
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
EHE-Tools (D:)
Network
Name
Date modified
Type
Size
cgiparam.ini 12/12/2019 4:01 AM Configuration sett... 1 KB
Client210.exe 12/12/2019 4:01 AM Application 522 KB
Editserver210.exe 12/12/2019 4:01 AM Application 236 KB
Loggedkeys.txt 12/12/2019 4:01 AM Text Document 1 KB
pass.dll 12/12/2019 4:01 AM Application exten... 42 KB
readme.txt 12/12/2019 4:01 AM Text Document 4 KB
Savedkeys.txt 12/12/2019 4:01 AM Text Document 0 KB
Scanner.dll 12/12/2019 4:01 AM Application exten... 60 KB
Server210.exe 12/12/2019
theef.ini 12/12/2019
upx.exe 12/12/2019
zip.dll 12/12/2019
Theef v.2.10
Computer Information
Task Manager
Show hidden windows
Caption
Handle
Spy
12 items
1 item selected 522 KB
State: Shared


Manage
Theef
File
Home
Share
View
Application Tools
This PC › EHE-Tools (D:) › EHE-Tools › EHE Module 03 Information Security Threats and Vulnerability Assessment › Trojans Types › Remote Access Trojans (RAT) ›
Quick access
Desktop
Downloads
Documents
Pictures
.ssh
EHE Module 07 Wel
EHE-Tools
Music
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
EHE-Tools (D:)
Network
Name
Date modified
Type
Size
cgiparam.ini 12/12/2019 4:01 AM Configuration sett... 1 KB
Client210.exe 12/12/2019 4:01 AM Application 522 KB
Editserver210.exe 12/12/2019 4:01 AM Application 236 KB
Loggedkeys.txt 12/12/2019 4:01 AM Text Document 1 KB
pass.dll 12/12/2019 4:01 AM Application exten... 42 KB
readme.txt 12/12/2019 4:01 AM Text Document 4 KB
Savedkeys.txt 12/12/2019 4:01 AM Text Document 0 KB
Scanner.dll 12/12/2019 4:01 AM Application exten... 60 KB
Server210.exe 12/12/201
theef.ini 12/12/201
upx.exe 12/12/201
zip.dll 12/12/201
Theef v.2.10
Computer Information
Keylogger [Started]
8 Mhz)
Keylogger started.
12 items
1 item selected 522 KB
State: Shared
Type here to search

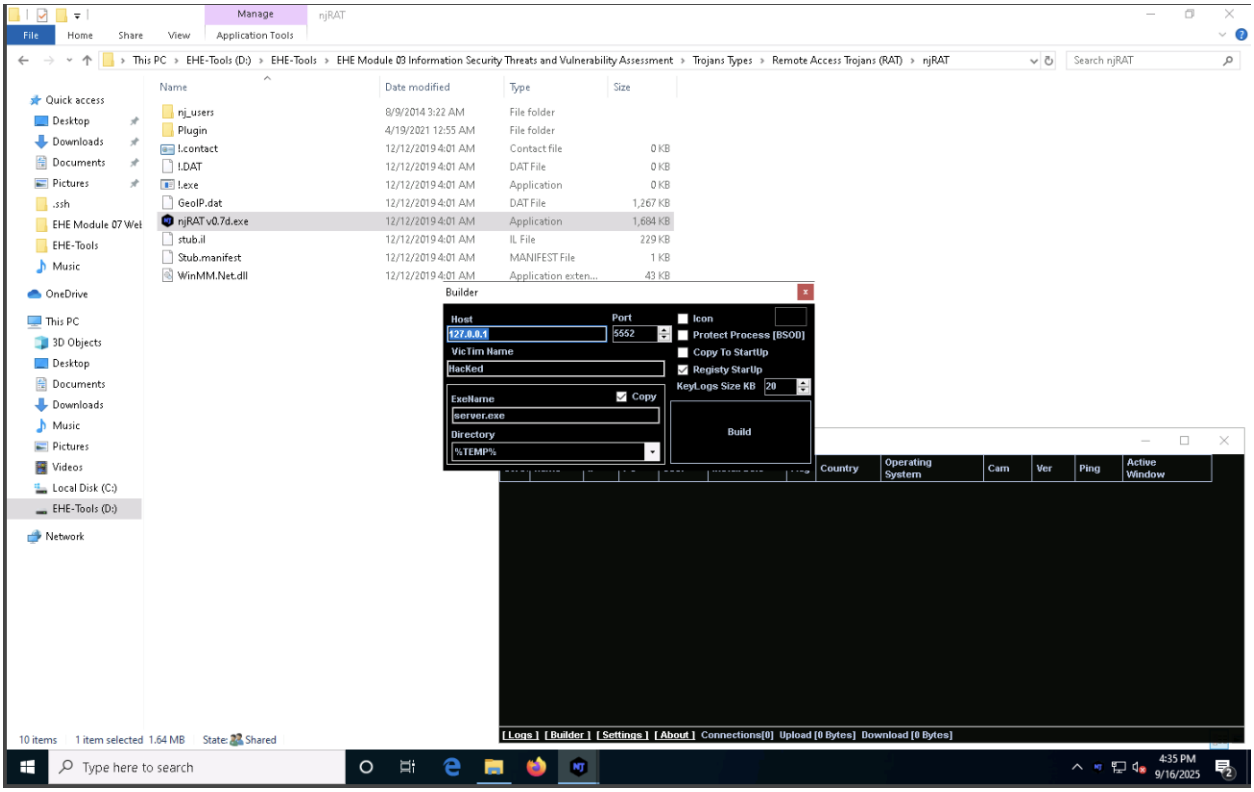


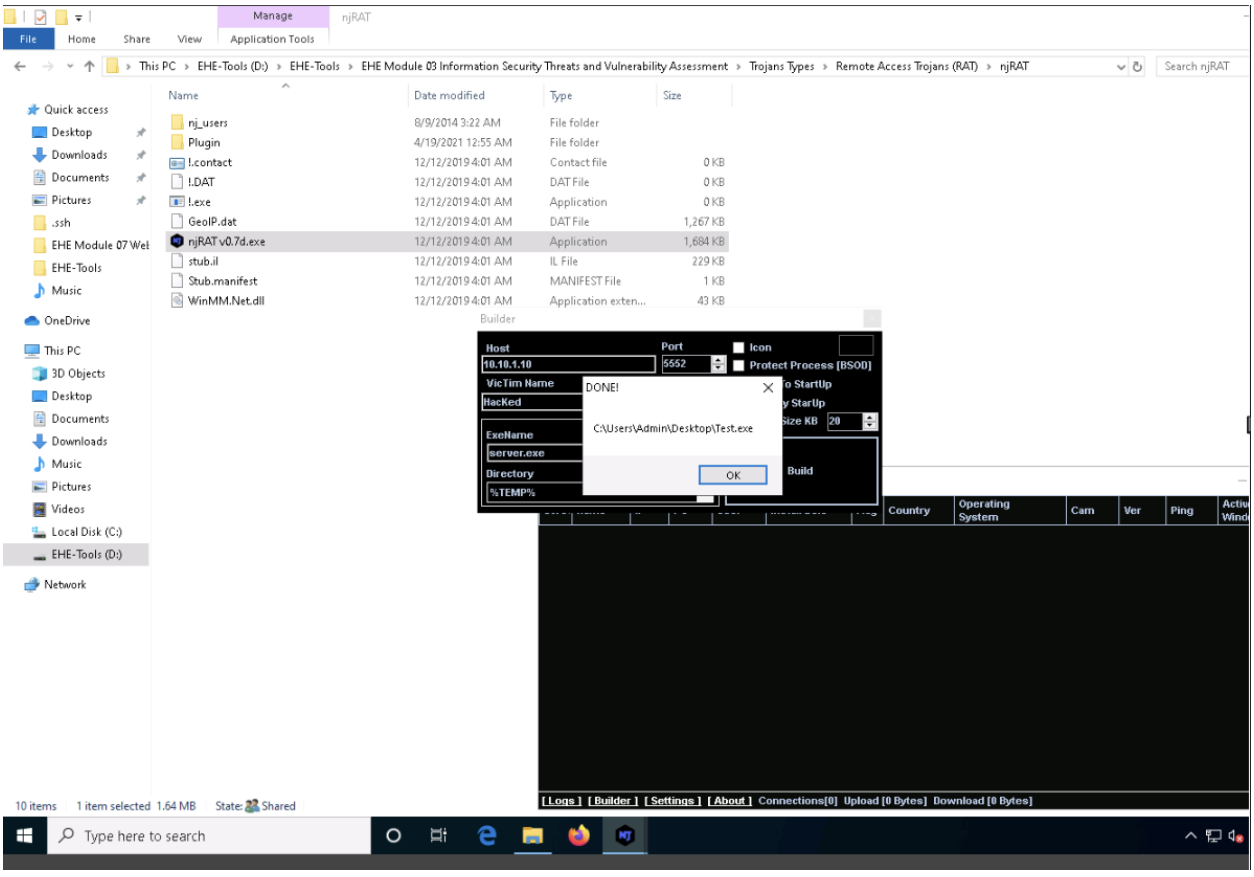
Task 2: Gain Control over a Victim Machine using the njRAT RAT Trojan

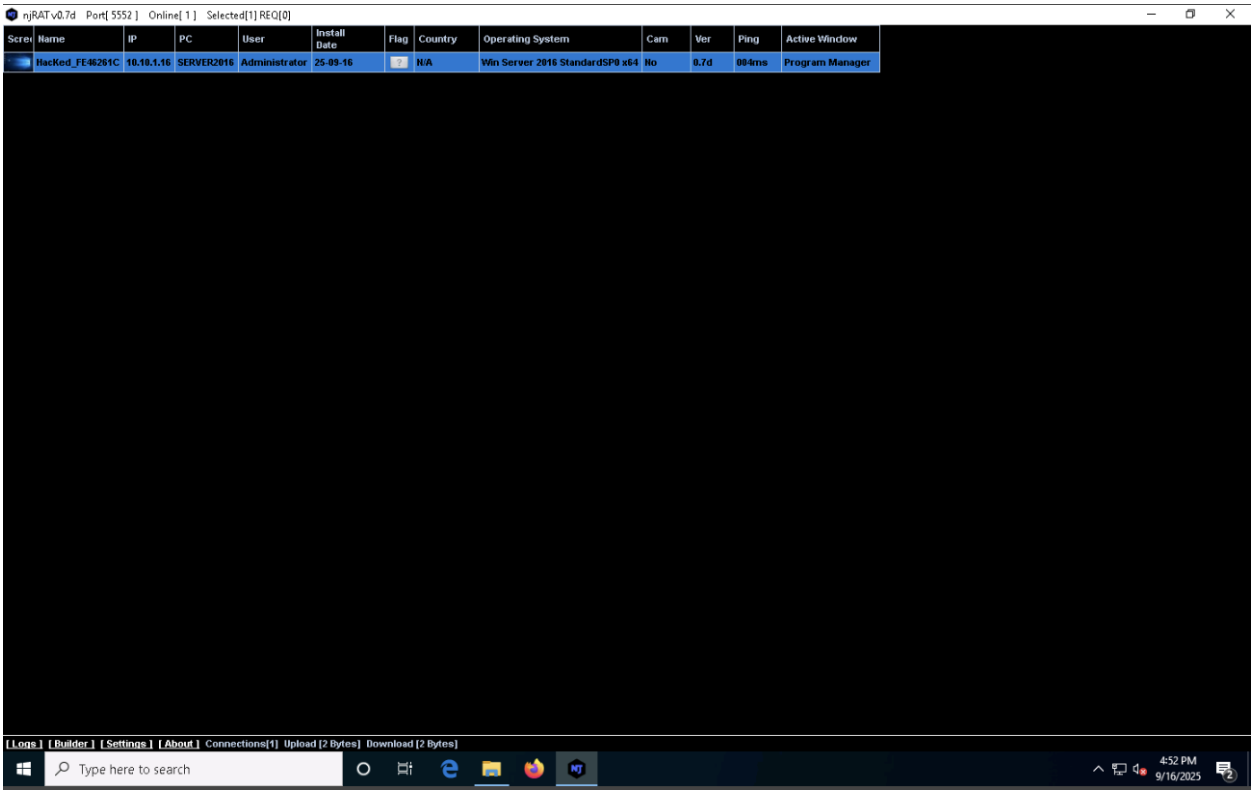
njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

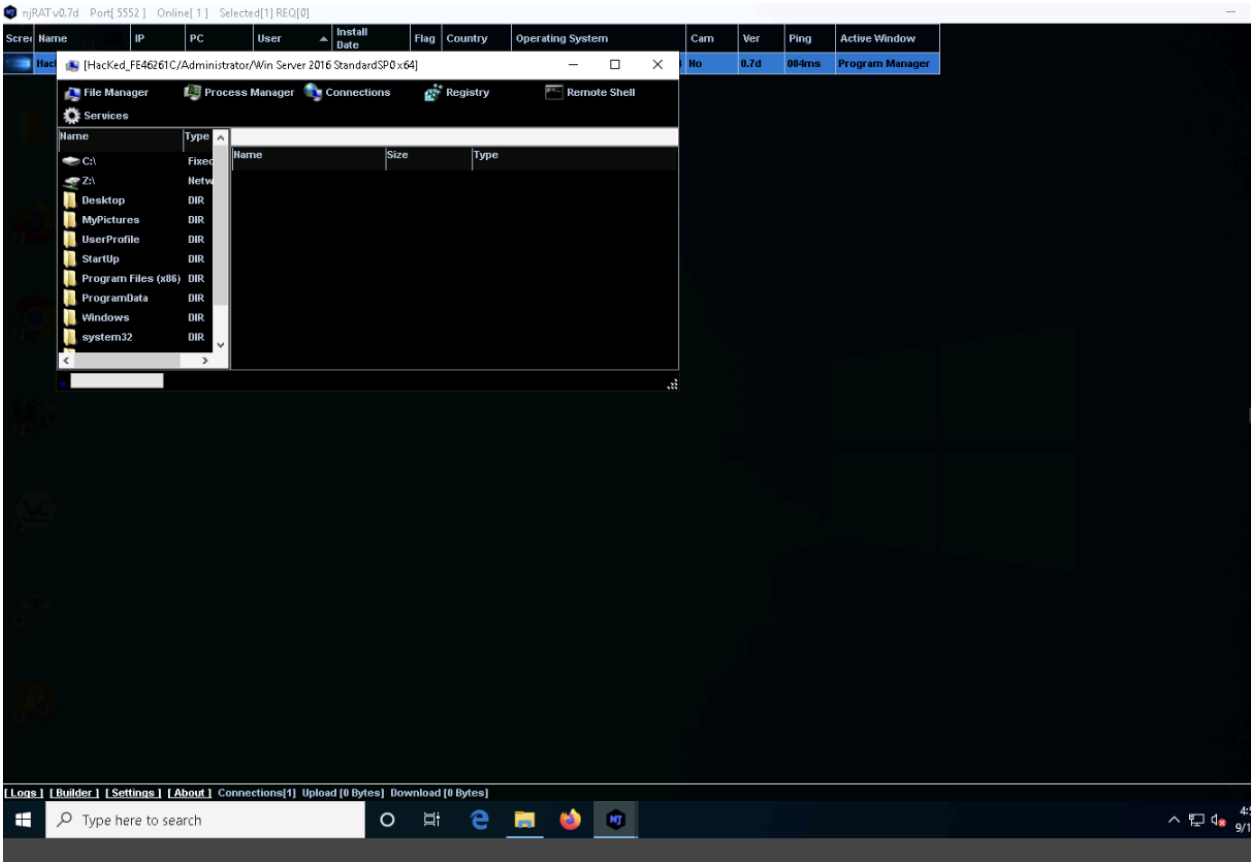
This RAT can be used to control Botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

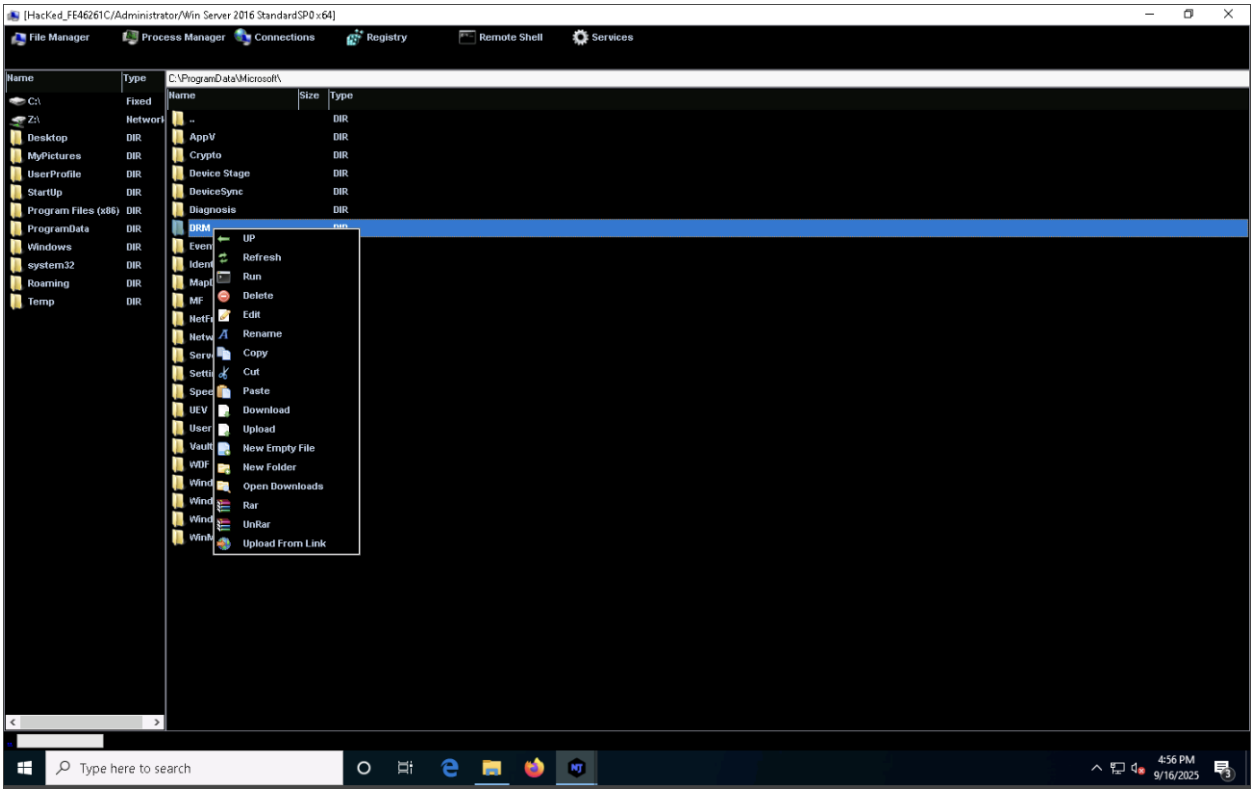
Here, we will use the njRAT Trojan to gain control over a victim machine.

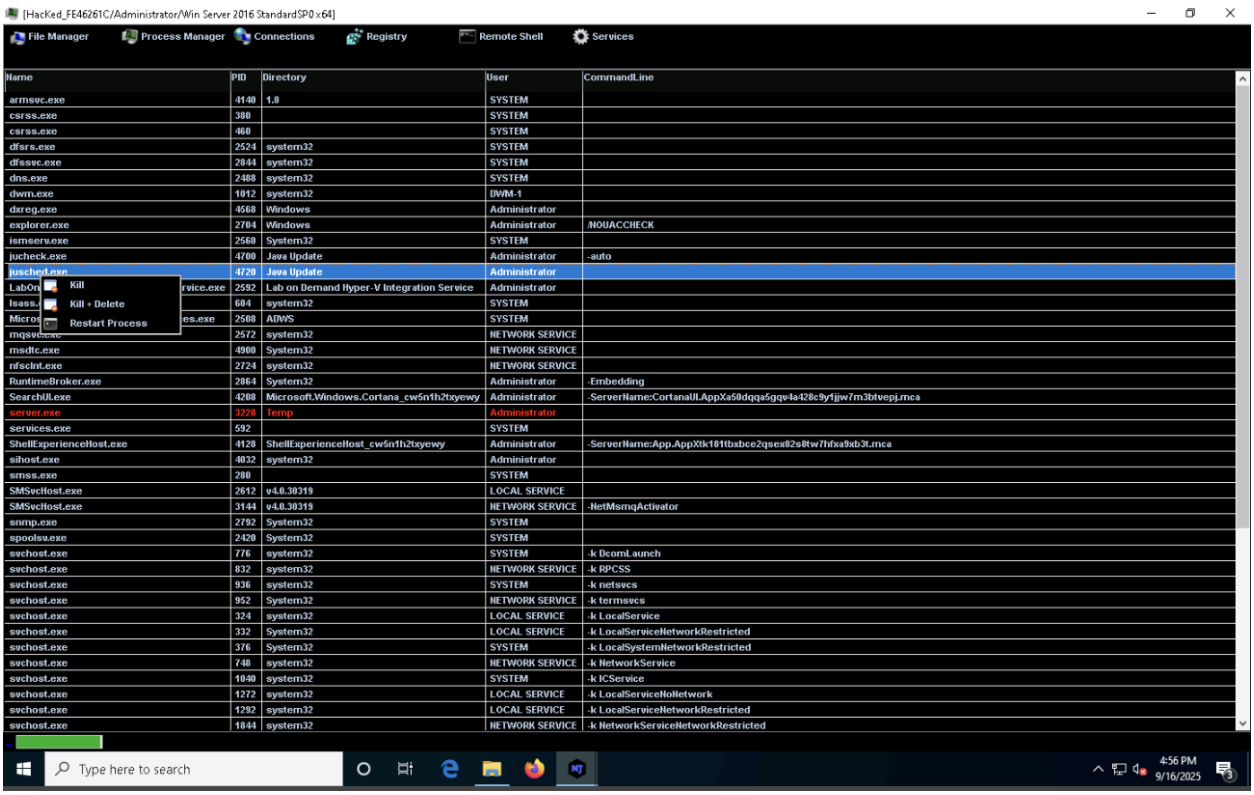

njRAT
Builder
Host
127.0.0.1
Port
5552
Icon
Protect Process [BSOD]
VicTim Name
HacKed
Copy To StartUp
Registy StartUp
KeyLogs Size KB
20
ExeName
server.exe
Copy
Directory
%TEMP%
Build
Country
Operating System
Cam
Ver
Ping
Active Window
[Logs] [Builder] [Settings] [About] Connections[0] Upload [0 Bytes] Download [0 Bytes]


njRAT
Builder
Host
10.10.1.10
Port
5552
Icon
Protect Process [BSOD]
VicTim Name
HacKed
DONE!
C:\Users\Admin\Desktop\Test.exe
OK
ExeName
server.exe
Directory
%TEMP%
Build
Country
Operating System
Cam
Ver
Ping
[Logs] [Builder] [Settings] [About] Connections[0] Upload [0 Bytes] Download [0 Bytes]

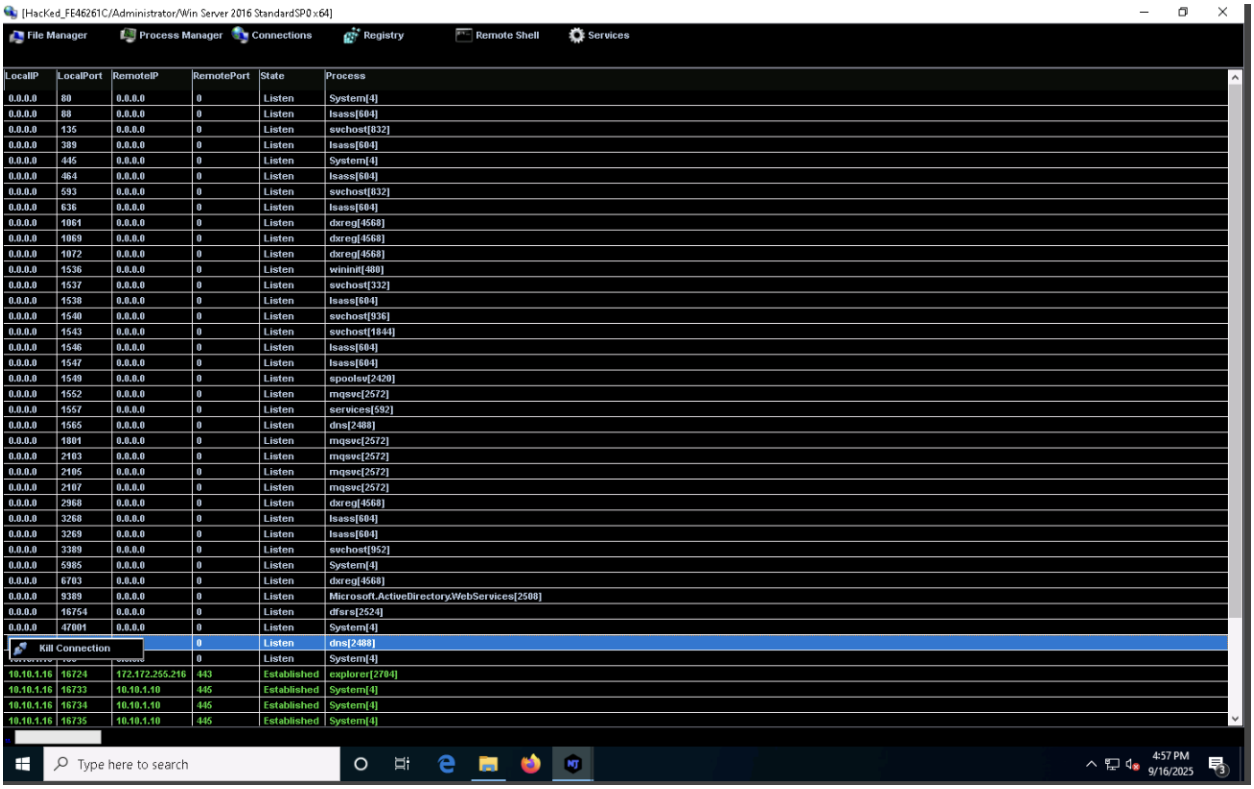

njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_FE46261C 10.10.1.16 SERVER2016 Administrator 25-09-16 N/A Win Server 2016 StandardSP0 x64 No 0.7d 084ms Program Manager
[Logs] [Builder] [Settings] [About] Connections[1] Upload [2 Bytes] Download [2 Bytes]
Type here to search
4:52 PM
9/16/2025

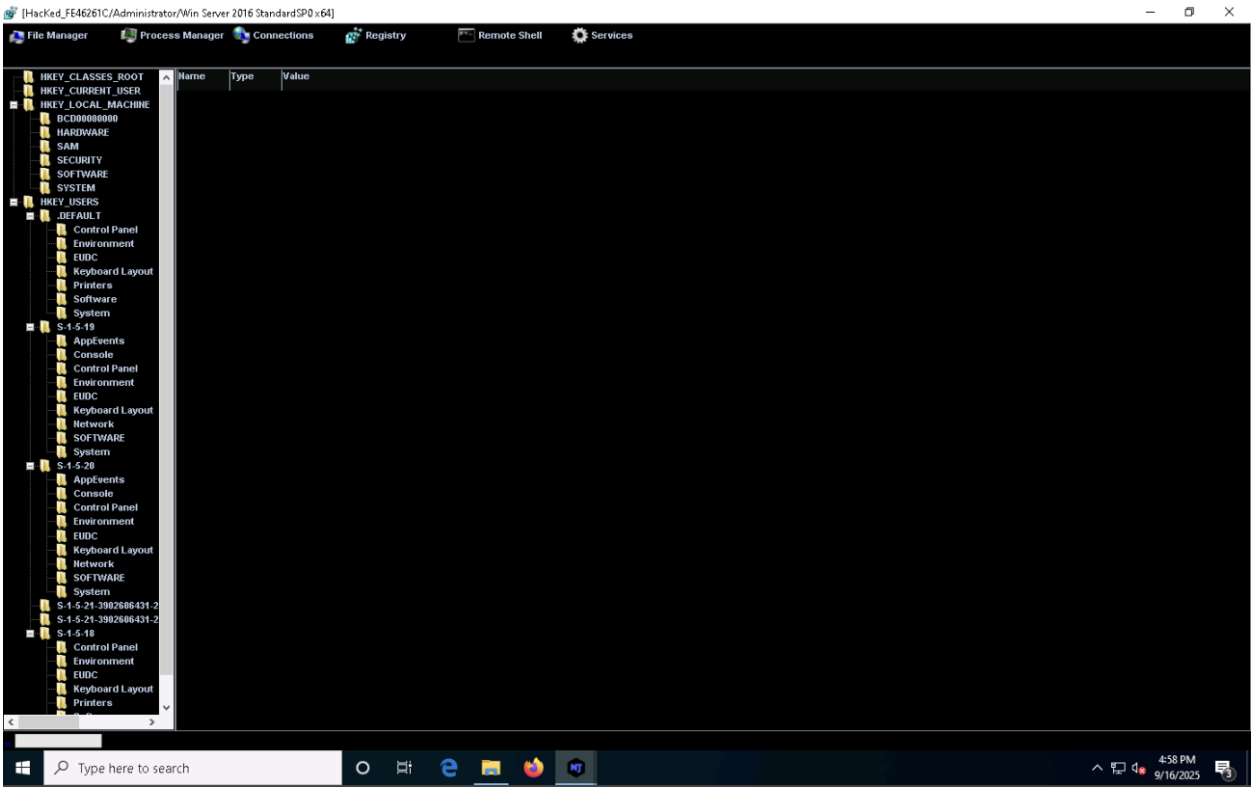

njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
[HacKed_FE46261C/Administrator/Win Server 2016 StandardSP0 x64]
No 0.7d 084ms Program Manager
File Manager
Process Manager
Connections
Registry
Remote Shell
Services
Name Type
C:\ Fixed
Z:\ Netw
Desktop DIR
MyPictures DIR
UserProfile DIR
StartUp DIR
Program Files (x86) DIR
ProgramData DIR
Windows DIR
system32 DIR
Name Size Type
[Logs] [Builder] [Settings] [About] Connections[1] Upload [0 Bytes] Download [0 Bytes]
Type here to search





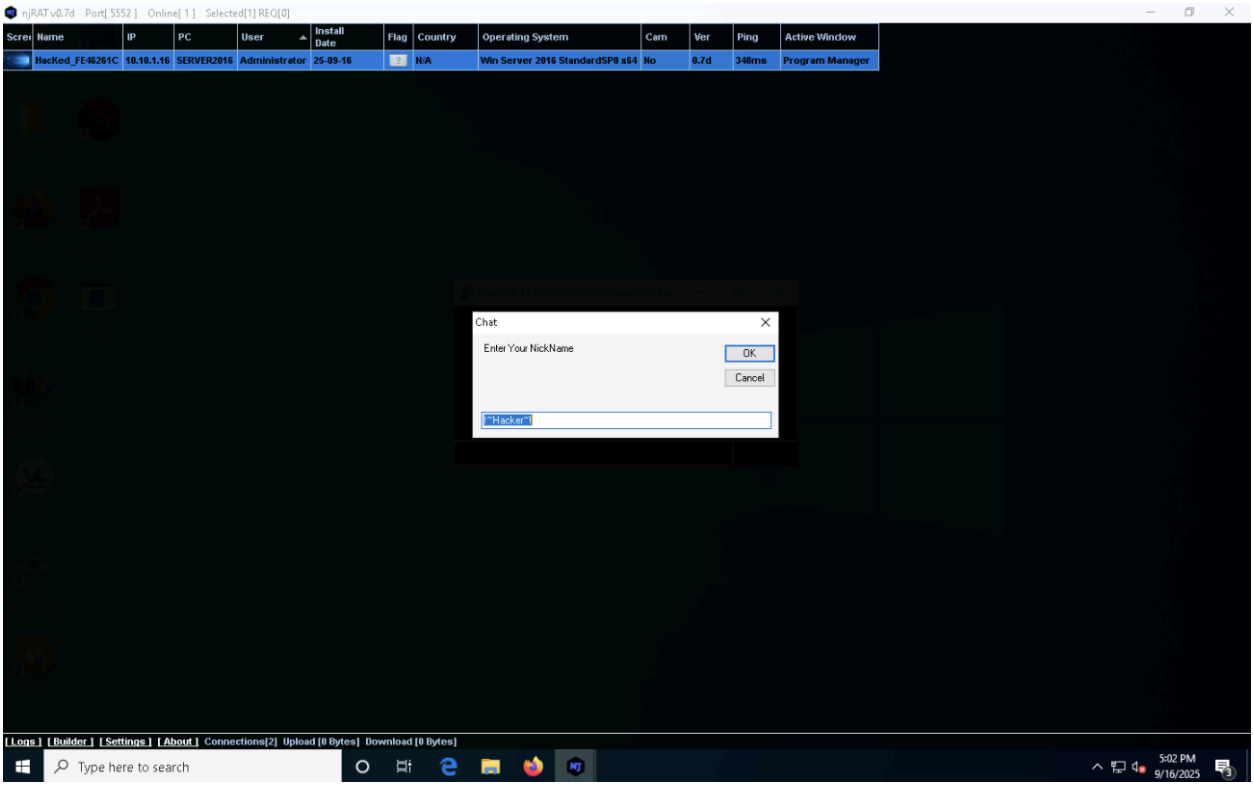
Name	PID	Directory	User	CommandLine
armsvc.exe	4140	1.0	SYSTEM	
csrss.exe	380		SYSTEM	
csrss.exe	460		SYSTEM	
dfsrs.exe	2524	system32	SYSTEM	
dfssvc.exe	2044	system32	SYSTEM	
dns.exe	2488	system32	SYSTEM	
dwm.exe	1012	system32	DWM-1	
dxreg.exe	4568	Windows	Administrator	
explorer.exe	2704	Windows	Administrator	/NOUACCHECK
ismserv.exe	2560	System32	SYSTEM	
jucheck.exe	4700	Java Update	Administrator	-auto
jusched.exe	4720	Java Update	Administrator	
LabOn	2592	Lab on Demand Hyper-V Integration Service	Administrator	
lsass.	604	system32	SYSTEM	
Micros	2508	ADWS	SYSTEM	
mqsvc.exe	2572	system32	NETWORK SERVICE	
msdtc.exe	4900	System32	NETWORK SERVICE	
nfsclnt.exe	2724	system32	NETWORK SERVICE	
RuntimeBroker.exe	2864	System32	Administrator	-Embedding
SearchUI.exe	4208	Microsoft.Windows.Cortana_cw5n1h2txyewy	Administrator	-ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca
server.exe	3228	Temp	Administrator	
services.exe	592		SYSTEM	
ShellExperienceHost.exe	4128	ShellExperienceHost_cw5n1h2txyewy	Administrator	-ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca
sihost.exe	4032	system32	Administrator	
smss.exe	280		SYSTEM	
SMSvcHost.exe	2612	v4.0.30319	LOCAL SERVICE	
SMSvcHost.exe	3144	v4.0.30319	NETWORK SERVICE	-NetMsmqActivator
snmp.exe	2792	System32	SYSTEM	
spoolsv.exe	2420	System32	SYSTEM	
svchost.exe	776	system32	SYSTEM	-k DcomLaunch
svchost.exe	832	system32	NETWORK SERVICE	-k RPCSS
svchost.exe	936	system32	SYSTEM	-k netsvcs
svchost.exe	952	System32	NETWORK SERVICE	-k termsvcs
svchost.exe	324	system32	LOCAL SERVICE	-k LocalService
svchost.exe	332	System32	LOCAL SERVICE	-k LocalServiceNetworkRestricted
svchost.exe	376	System32	SYSTEM	-k LocalSystemNetworkRestricted
svchost.exe	748	system32	NETWORK SERVICE	-k NetworkService
svchost.exe	1040	system32	SYSTEM	-k ICService
svchost.exe	1272	system32	LOCAL SERVICE	-k LocalServiceNoNetwork
svchost.exe	1292	system32	LOCAL SERVICE	-k LocalServiceNetworkRestricted
svchost.exe	1844	system32	NETWORK SERVICE	-k NetworkServiceNetworkRestricted

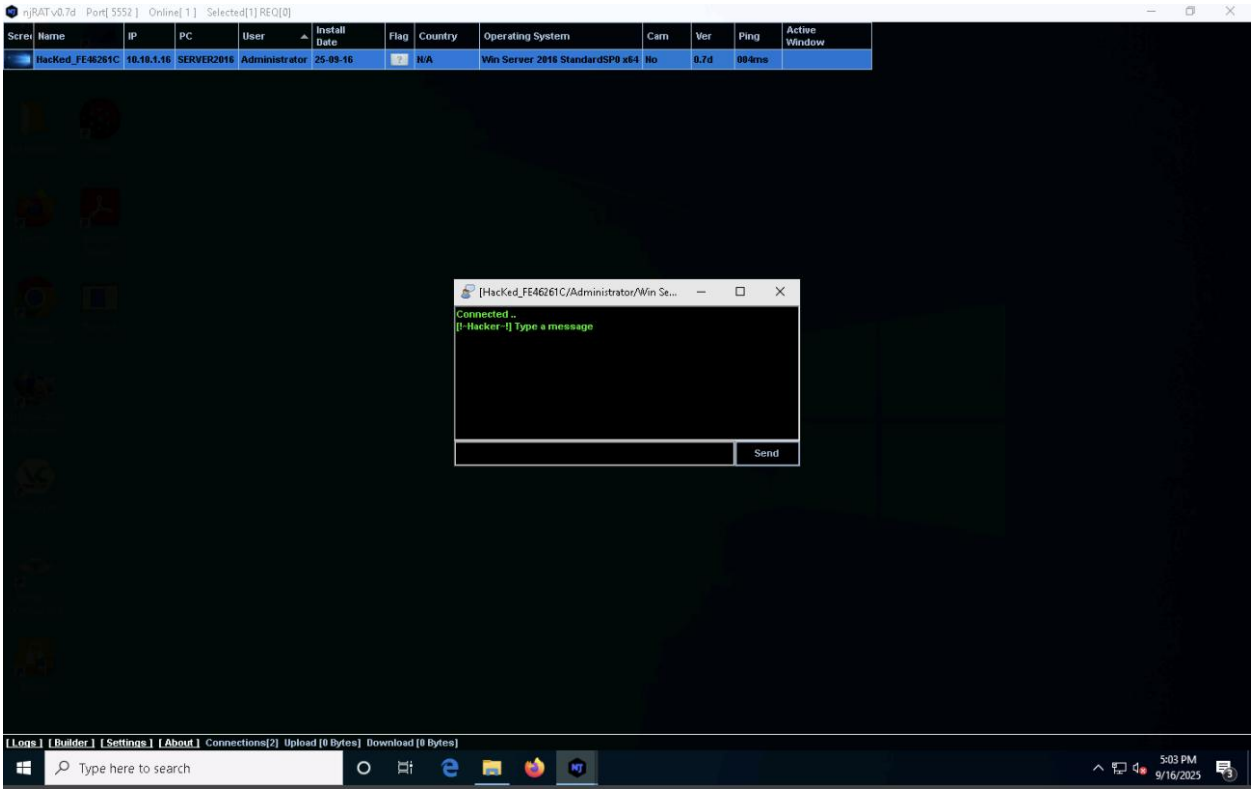


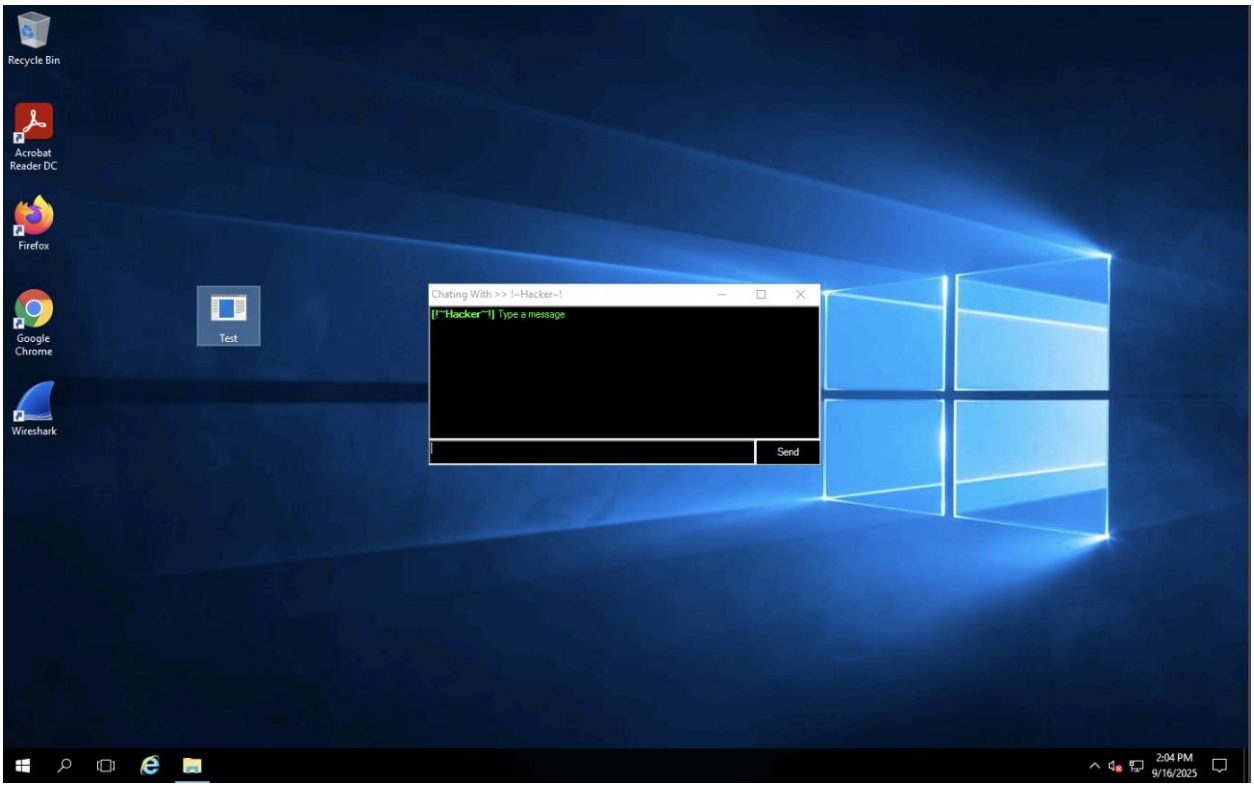


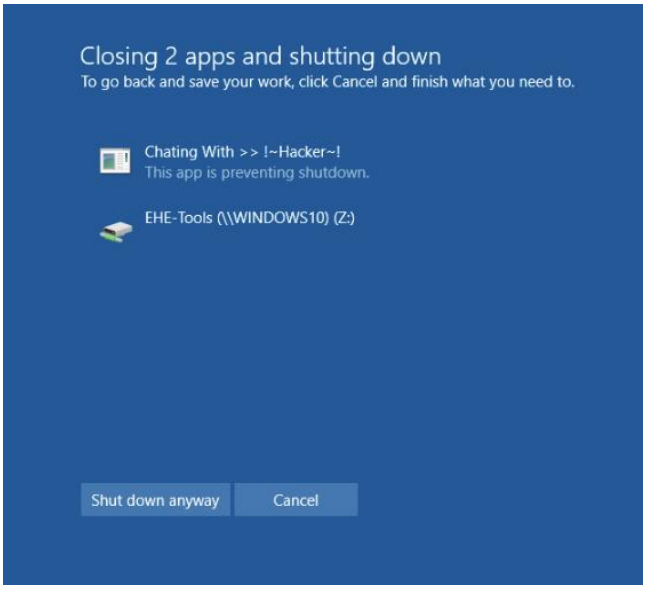
Observation: Opened Remote Shell from the njRAT client interface. The shell displayed a Windows Server 2016 command prompt environment, but the interface did not accept

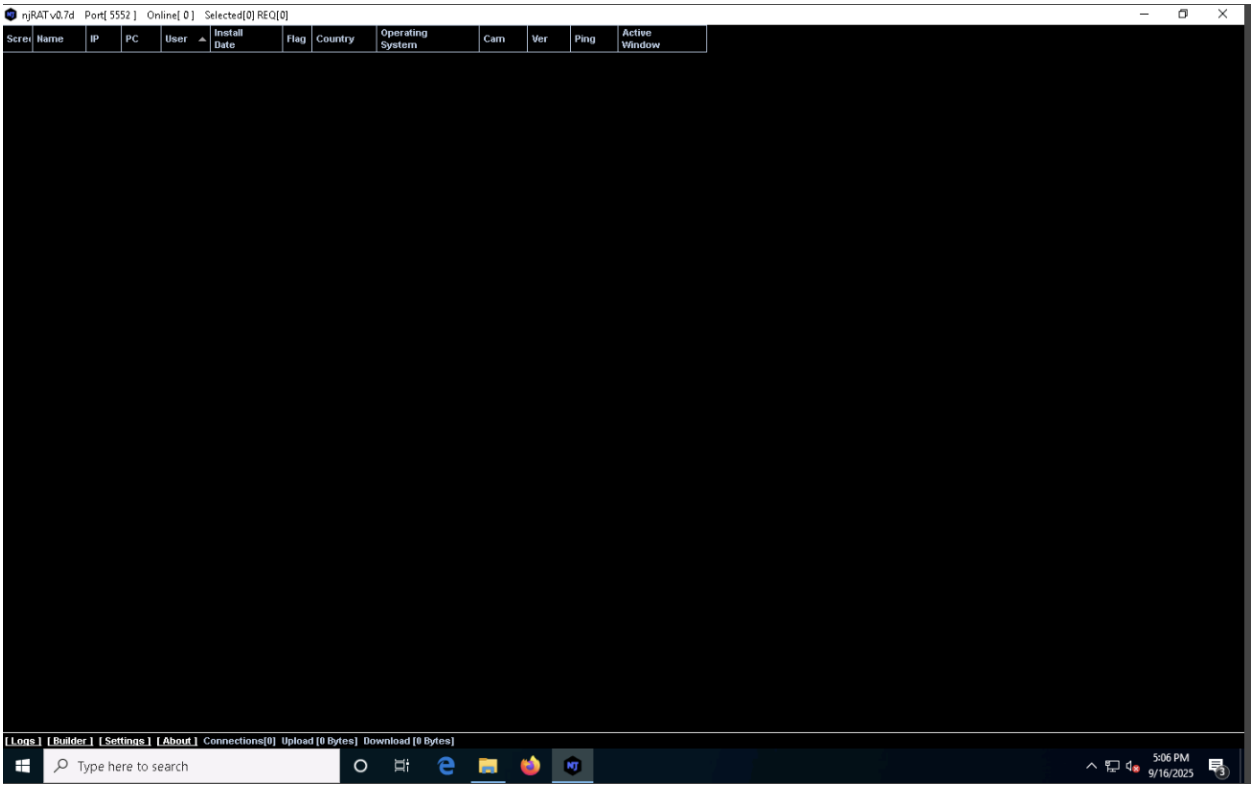
input. The expected command (ipconfig /all) could not be entered. This indicates that the lab environment provides a visual demonstration of RAT capabilities but restricts live interaction for security reasons.

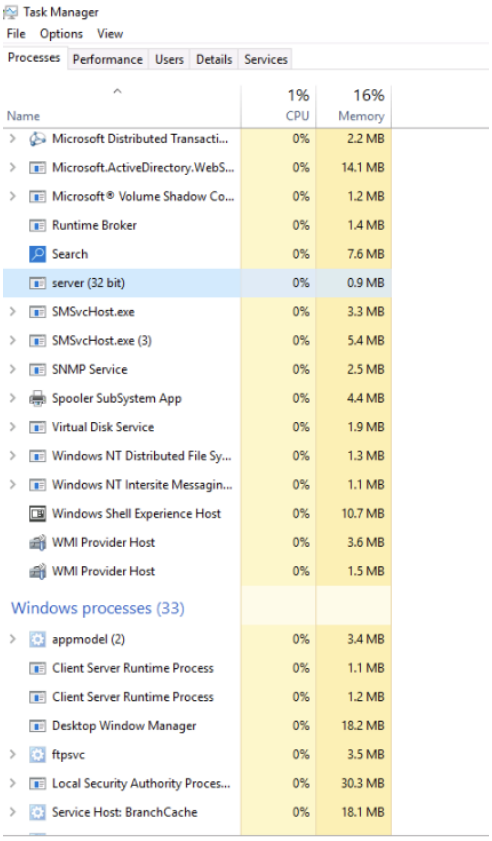



njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_FE46261C 10.10.1.16 SERVER2016 Administrator 25-09-16 N/A Win Server 2016 StandardSP0 x64 No 0.7d 884ms
[HacKed_FE46261C/Administrator/Win Se...
Connected ..
[!~Hacker~!] Type a message
Send
[Logs] [Builder] [Settings] [About] Connections[2] Upload [0 Bytes] Download [0 Bytes]
Type here to search
5:03 PM
9/16/2025


Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
Test
Chating With >> !~Hacker~!
[!~Hacker~!] Type a message
Send
2:04 PM
9/16/2025


Closing 2 apps and shutting down
To go back and save your work, click Cancel and finish what you need to.
Chating With >> !~Hacker~!
This app is preventing shutdown.
EHE-Tools (\\WINDOWS10) (Z:)
Shut down anyway
Cancel


njRAT v0.7d
Port[5552]
Online[0]
Selected[0] REQ[0]
Scree
Name
IP
PC
User
Install Date
Flag
Country
Operating System
Cam
Ver
Ping
Active Window
[Logs] [Builder] [Settings] [About] Connections[0] Upload [0 Bytes] Download [0 Bytes]
Type here to search
5:06 PM
9/16/2025



Lab 2: Create a Virus to Infect the Target System

Lab Scenario

Viruses are the scourges of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce. Therefore, attackers design every virus code in such a manner that the virus replicates itself n number of times, where n is a number specified by the attacker.

Virus reproduces its own code while enclosing other executables, and spreads throughout the computer. Viruses can spread the infection by damaging files in a file system. Some viruses reside in the memory and may infect programs through the boot sector. A virus can also be in an encrypted form.

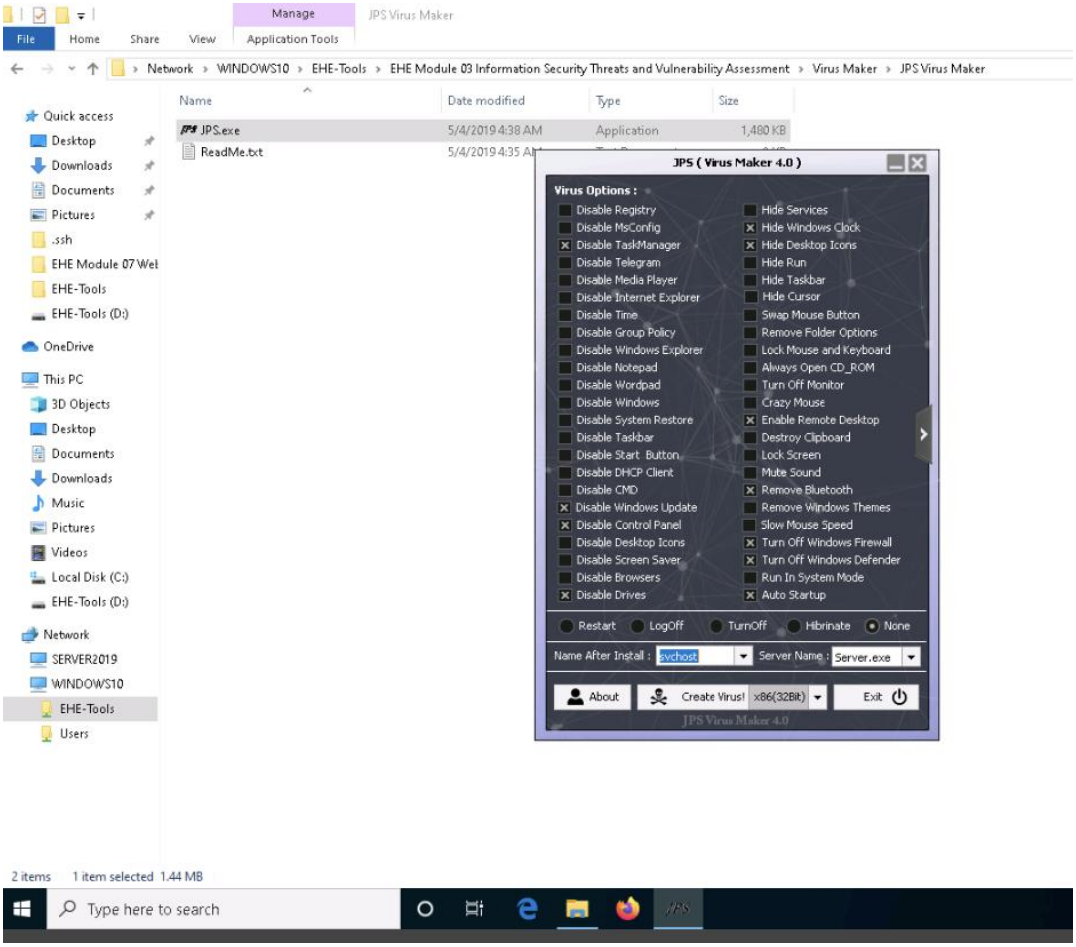
Lab Objectives

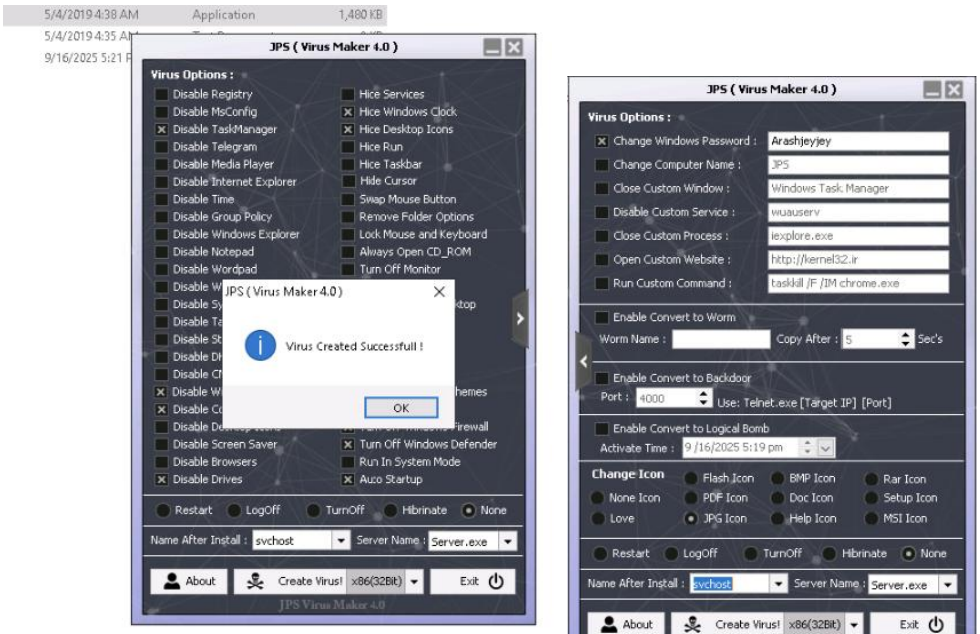
- Create a Virus using the JPS Virus Maker Tool and Infect the Target System

Task 1: Create a Virus using the JPS Virus Maker Tool and Infect the Target System

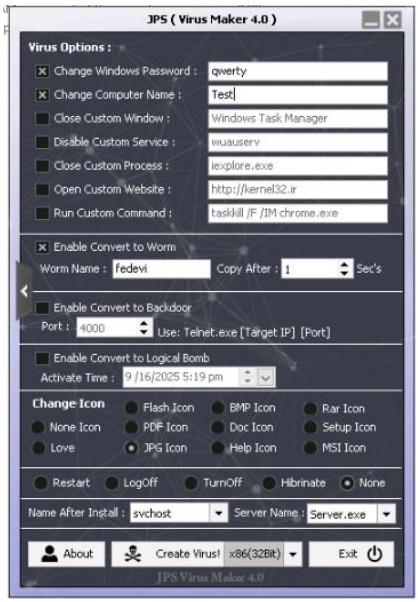
The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-

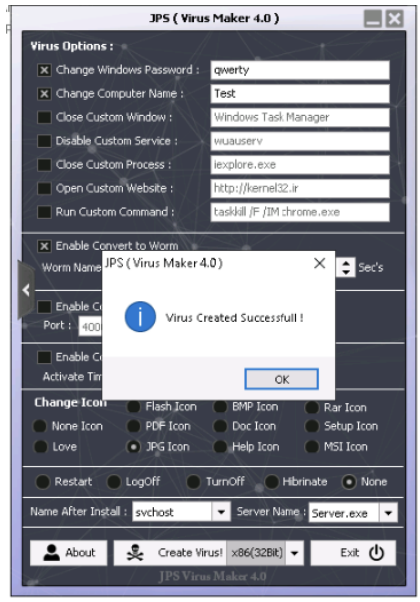
start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows. We can use the JPS Virus Maker Tool as a proof of concept to audit perimeter security controls in an organization.

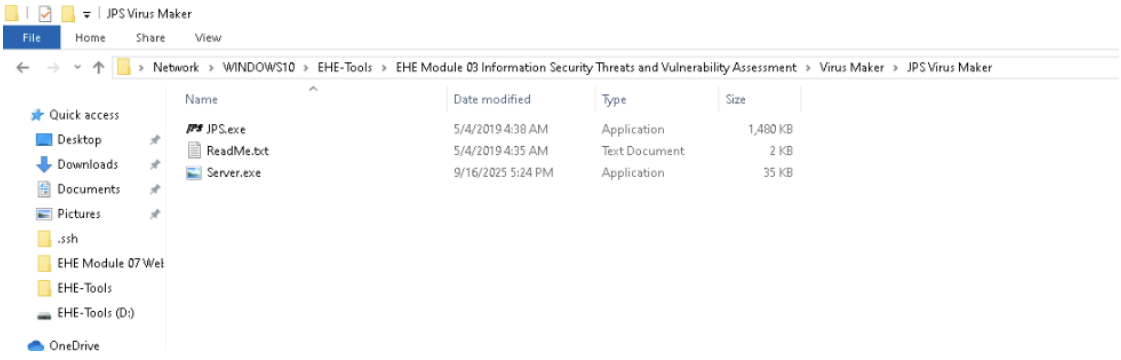


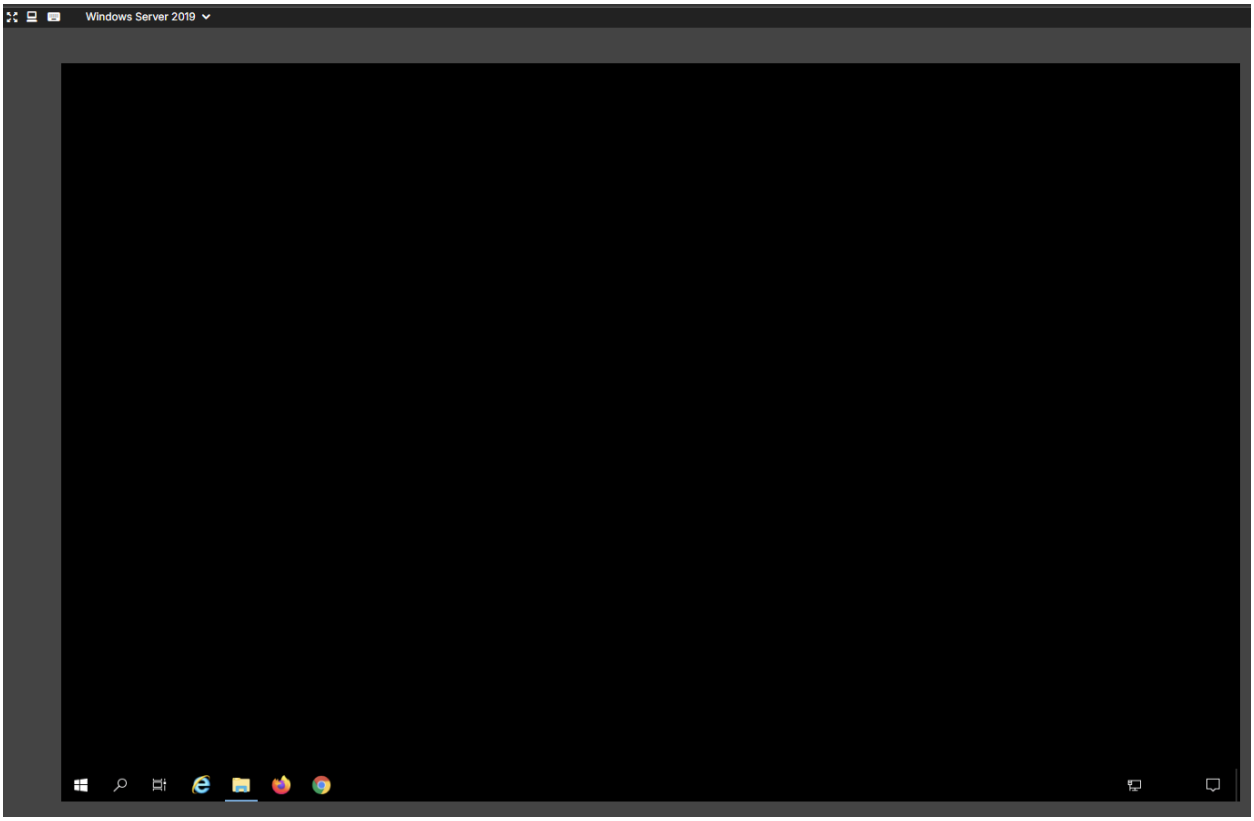

5/4/2019 4:38 AM Application 1,480 KB
5/4/2019 4:35 AM
9/16/2025 5:21 P
JPS (Virus Maker 4.0)
Virus Options :
Disable Registry
Disable MsConfig
Disable TaskManager
Disable Telegram
Disable Media Player
Disable Internet Explorer
Disable Time
Disable Group Policy
Disable Windows Explorer
Disable Notepad
Disable Wordpad
Hide Services
Hide Windows Clock
Hide Desktop Icons
Hide Run
Hide Taskbar
Hide Cursor
Swap Mouse Button
Remove Folder Options
Lock Mouse and Keyboard
Always Open CD_ROM
Turn Off Monitor
Disable Screen Saver
Disable Browsers
Disable Drives
Turn Off Windows Defender
Run In System Mode
Auto Startup
JPS (Virus Maker 4.0)
Virus Created Successfull !
OK
Restart
LogOff
TurnOff
Hibrinate
None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus!
x86(32Bit)
Exit
JPS Virus Maker 4.0

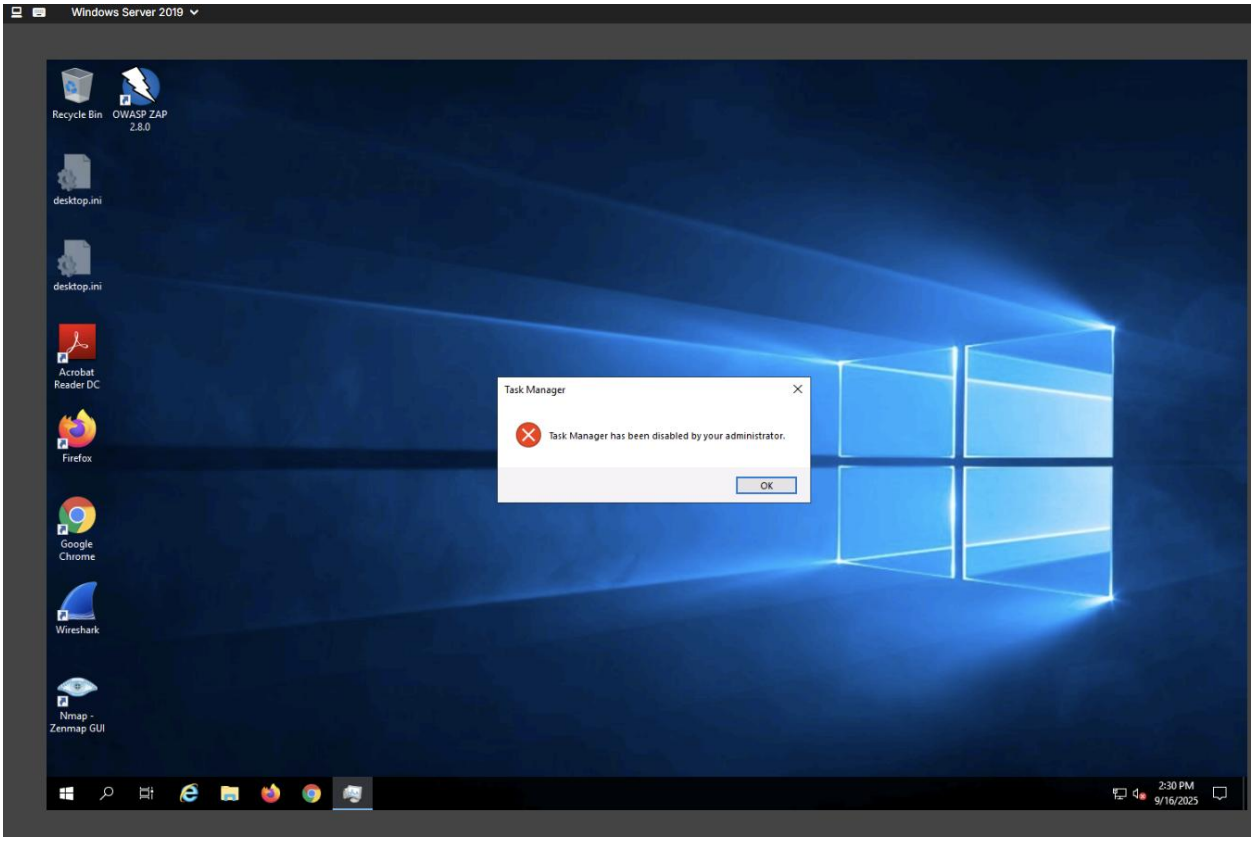
JPS (Virus Maker 4.0)
Virus Options :
Change Windows Password : Arashjeyjey
Change Computer Name : JPS
Close Custom Window : Windows Task Manager
Disable Custom Service : wuauserv
Close Custom Process : iexplore.exe
Open Custom Website : http://kernel32.ir
Run Custom Command : taskkill /F /IM chrome.exe
Enable Convert to Worm
Worm Name :
Copy After : 5 Sec's
Enable Convert to Backdoor
Port : 4000
Use: Telnet.exe [Target IP] [Port]
Enable Convert to Logical Bomb
Activate Time : 9 /16/2025 5:19 pm
Change Icon
Flash Icon
BMP Icon
Rar Icon
None Icon
PDF Icon
Doc Icon
Setup Icon
Love
JPG Icon
Help Icon
MSI Icon
Restart
LogOff
TurnOff
Hibrinate
None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus!
x86(32Bit)
Exit
JPS Virus Maker 4.0


JPS (Virus Maker 4.0)
Virus Options :
Change Windows Password : qwerty
Change Computer Name : Test
Close Custom Window : Windows Task Manager
Disable Custom Service : wuauserv
Close Custom Process : iexplore.exe
Open Custom Website : http://kernel32.ir
Run Custom Command : taskkill /F /IM chrome.exe
Enable Convert to Worm
Worm Name : fedevi
Copy After : 1 Sec's
Enable Convert to Backdoor
Port : 4000
Use: Telnet.exe [Target IP] [Port]
Enable Convert to Logical Bomb
Activate Time : 9 /16/2025 5:19 pm
Change Icon
Flash Icon
BMP Icon
Rar Icon
None Icon
PDF Icon
Doc Icon
Setup Icon
Love
JPG Icon
Help Icon
MSI Icon
Restart
LogOff
TurnOff
Hibrinate
None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus!
x86(32Bit)
Exit
JPS Virus Maker 4.0


JPS (Virus Maker 4.0)
Virus Options :
Change Windows Password : qwerty
Change Computer Name : Test
Close Custom Window : Windows Task Manager
Disable Custom Service : wuauserv
Close Custom Process : iexplore.exe
Open Custom Website : http://kernel32.ir
Run Custom Command : taskkill /F /IM chrome.exe
Enable Convert to Worm
Sec's
JPS (Virus Maker 4.0)
Virus Created Successfull !
OK
Change Icon
Flash Icon
BMP Icon
Rar Icon
None Icon
PDF Icon
Doc Icon
Setup Icon
Love
JPG Icon
Help Icon
MSI Icon
Restart
LogOff
TurnOff
Hibrinate
None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus!
x86(32Bit)
Exit
JPS Virus Maker 4.0


JPS Virus Maker
File
Home
Share
View
Network › WINDOWS10 › EHE-Tools › EHE Module 03 Information Security Threats and Vulnerability Assessment › Virus Maker › JPS Virus Maker
Quick access
Desktop
Downloads
Documents
Pictures
.ssh
EHE Module 07 Wel
EHE-Tools
EHE-Tools (D:)
OneDrive
Name
Date modified
Type
Size
JPS.exe 5/4/2019 4:38 AM Application 1,480 KB
ReadMe.txt 5/4/2019 4:35 AM Text Document 2 KB
Server.exe 9/16/2025 5:24 PM Application 35 KB


Windows Server 2019



Lab 3: Perform Vulnerability Assessment to Identify Security Vulnerabilities in the Target System or Network

Lab Scenario

The information gathered in the previous labs might not be sufficient to reveal potential vulnerabilities of the target: there could be more information available that may help in finding loopholes. As an ethical hacker, you should look for as much information as possible using all available tools. This lab will demonstrate other information that you can extract from the target using various vulnerability assessment tools.

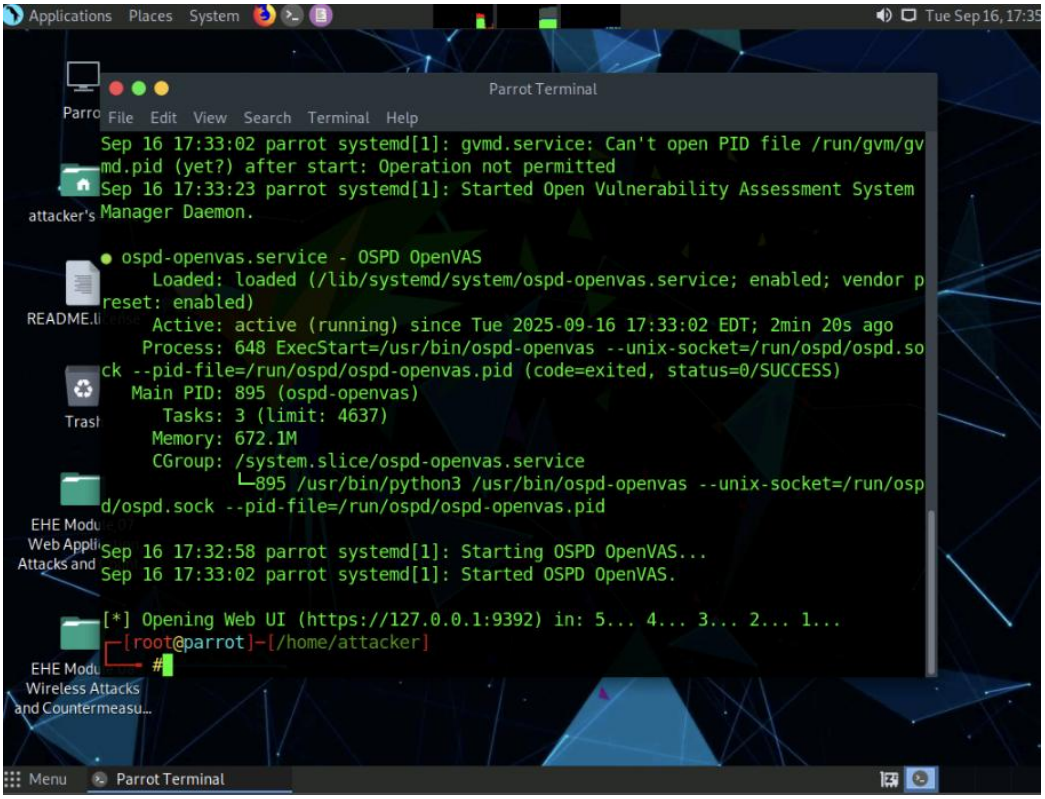
Lab Objectives

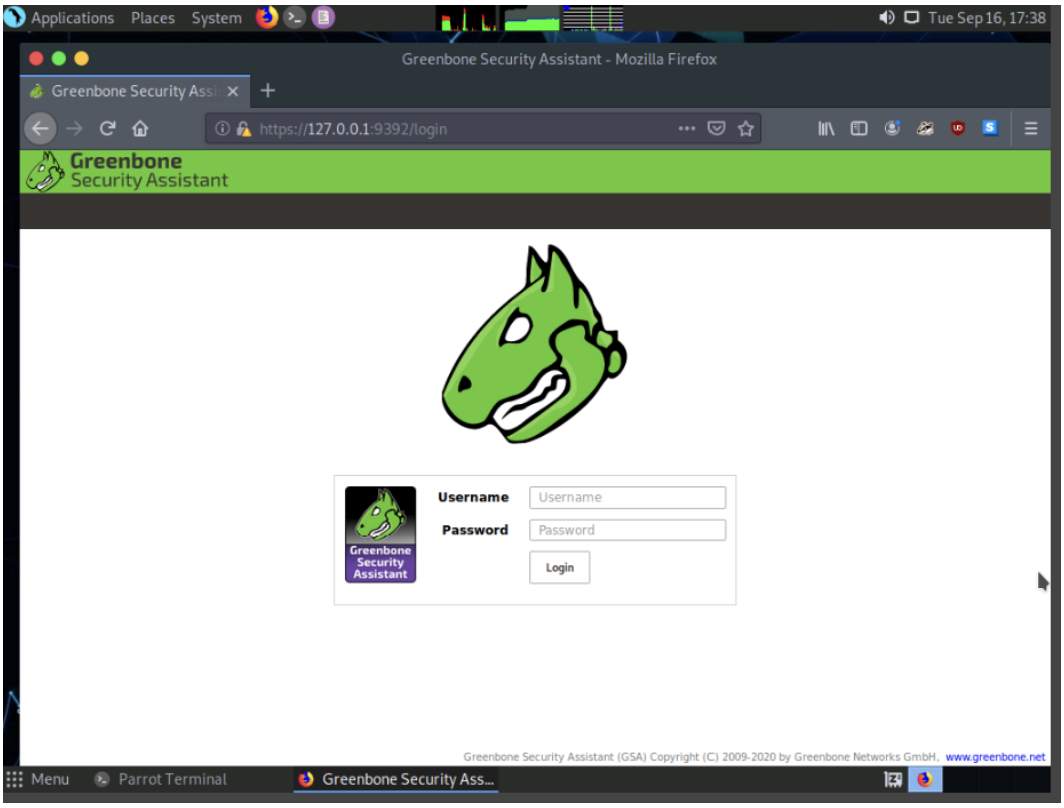
- Perform Vulnerability Analysis using OpenVAS

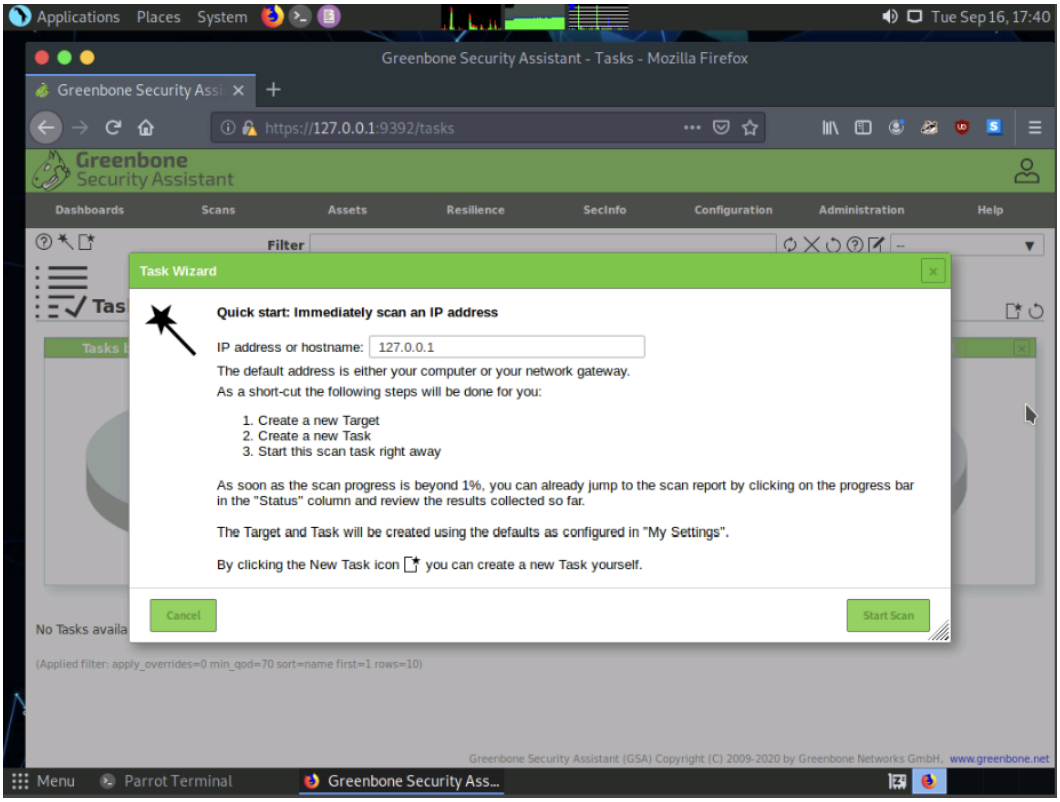
Task 1: Perform Vulnerability Analysis using OpenVAS

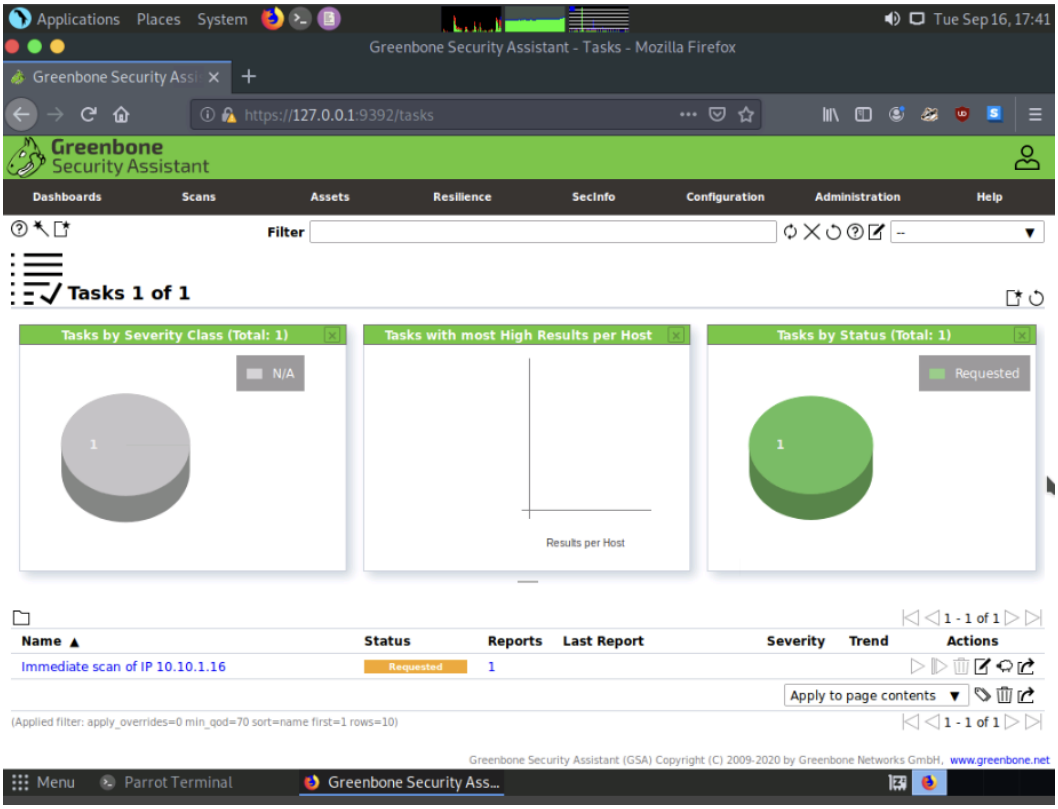
OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test. The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)-over 50,000 in total.

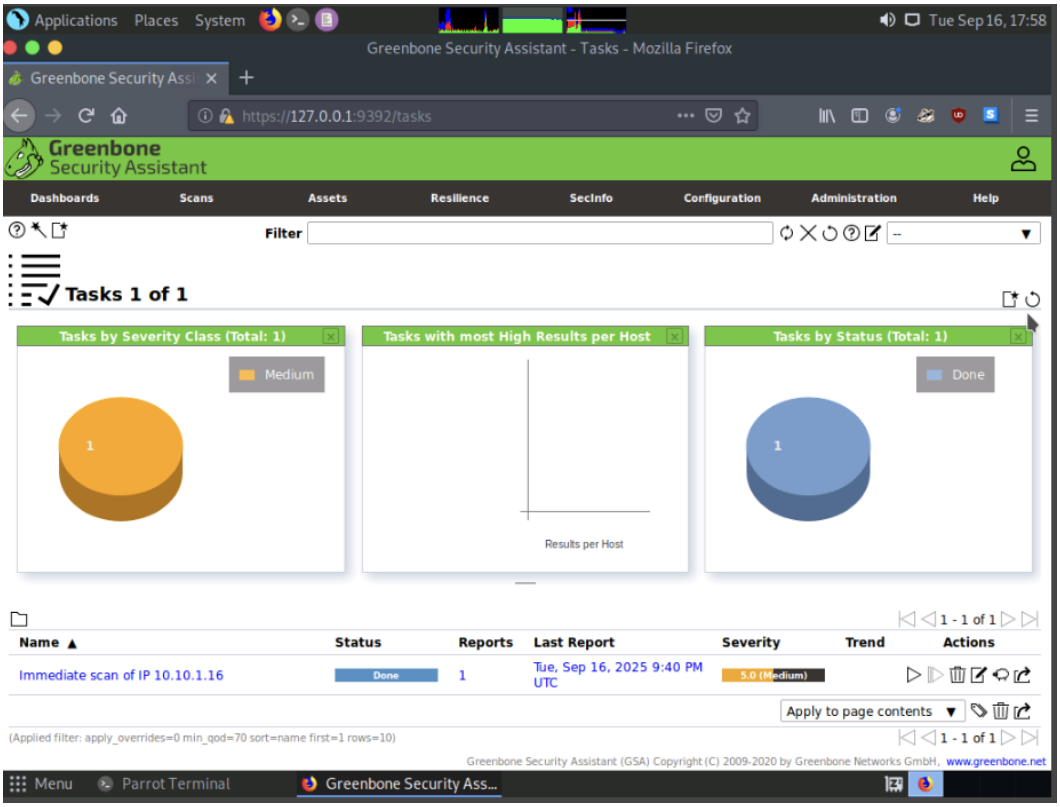
Here, we will perform a vulnerability analysis using OpenVAS.

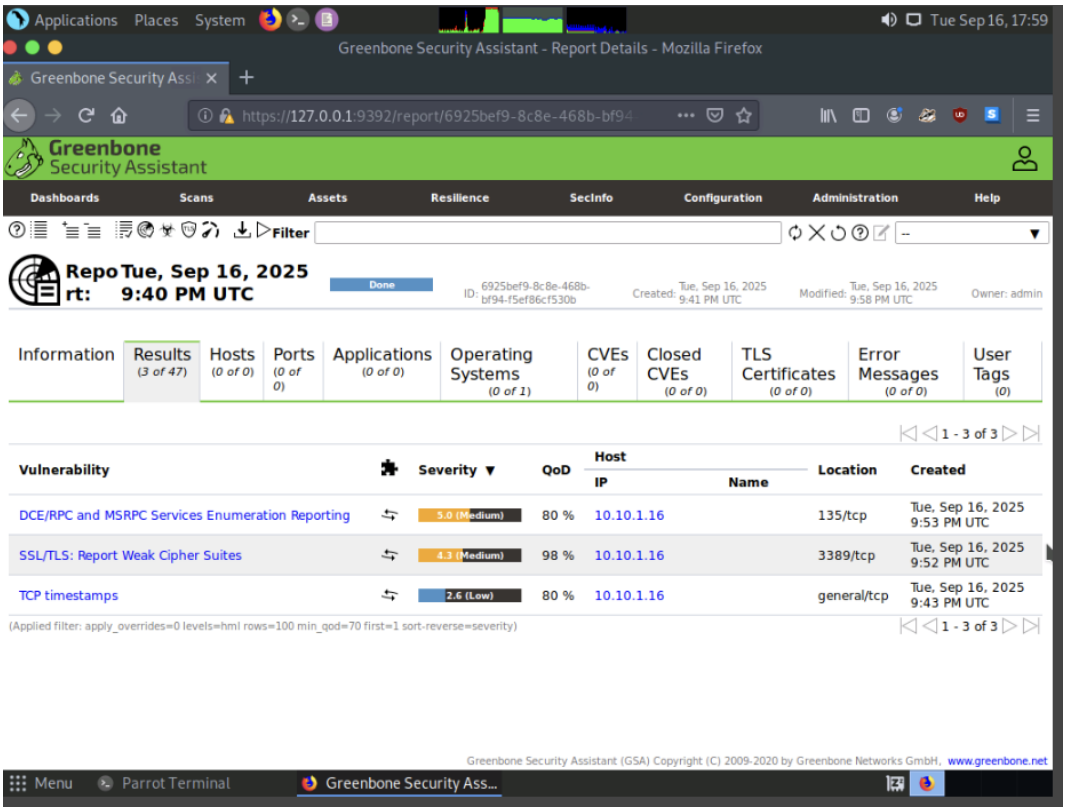


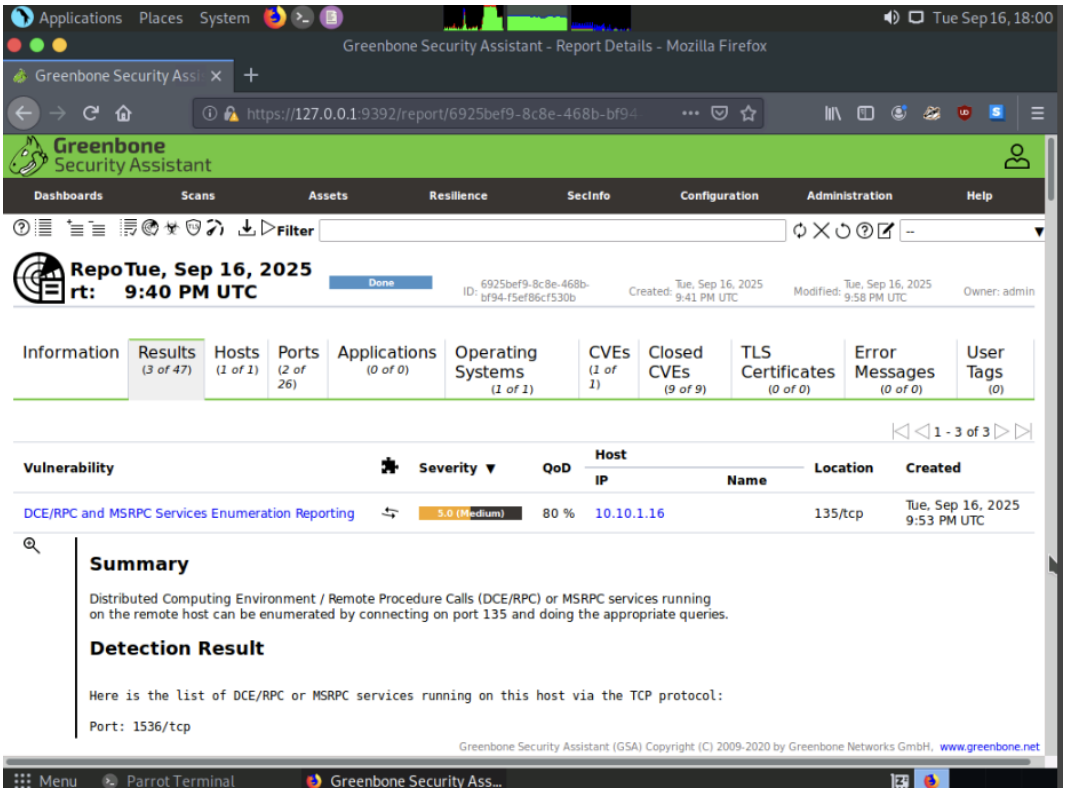

Applications Places System
Tue Sep 16, 17:38
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/login
Greenbone
Security Assistant
Username
Password
Login
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net
Menu
Parrot Terminal
Greenbone Security Ass...


Applications Places System
Tue Sep 16, 17:40
Greenbone Security Assistant - Tasks - Mozilla Firefox
https://127.0.0.1:9392/tasks
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Task Wizard
Quick start: Immediately scan an IP address
IP address or hostname: 127.0.0.1
The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:
1. Create a new Target
2. Create a new Task
3. Start this scan task right away
As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.
The Target and Task will be created using the defaults as configured in "My Settings".
By clicking the New Task icon you can create a new Task yourself.
Cancel
Start Scan
No Tasks availa
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net
Menu
Parrot Terminal
Greenbone Security Ass...


Applications Places System
Tue Sep 16, 17:41
Greenbone Security Assistant - Tasks - Mozilla Firefox
https://127.0.0.1:9392/tasks
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
N/A
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 1)
Requested
1 - 1 of 1
Name Status Reports Last Report Severity Trend Actions
Immediate scan of IP 10.10.1.16
Requested
1
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net
Menu
Parrot Terminal
Greenbone Security Ass...


Applications Places System
Tue Sep 16, 17:58
Greenbone Security Assistant - Tasks - Mozilla Firefox
https://127.0.0.1:9392/tasks
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
Medium
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 1)
Done
1 - 1 of 1
Name Status Reports Last Report Severity Trend Actions
Immediate scan of IP 10.10.1.16
Done
1
Tue, Sep 16, 2025 9:40 PM UTC
5.0 (Medium)
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net
Menu
Parrot Terminal
Greenbone Security Ass...


Applications Places System
Tue Sep 16, 17:59
Greenbone Security Assistant - Report Details - Mozilla Firefox
https://127.0.0.1:9392/report/6925bef9-8c8e-468b-bf94
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Report: Tue, Sep 16, 2025 9:40 PM UTC
Done
ID: 6925bef9-8c8e-468b-bf94-f5ef86cf530b
Created: Tue, Sep 16, 2025 9:41 PM UTC
Modified: Tue, Sep 16, 2025 9:58 PM UTC
Owner: admin
Information Results (3 of 47) Hosts (0 of 0) Ports (0 of 0) Applications (0 of 0) Operating Systems (0 of 1) CVEs (0 of 0) Closed CVEs (0 of 0) TLS Certificates (0 of 0) Error Messages (0 of 0) User Tags (0)
1 - 3 of 3
Vulnerability Severity QoD Host IP Name Location Created
DCE/RPC and MSRPC Services Enumeration Reporting 5.0 (Medium) 80 % 10.10.1.16 135/tcp Tue, Sep 16, 2025 9:53 PM UTC
SSL/TLS: Report Weak Cipher Suites 4.3 (Medium) 98 % 10.10.1.16 3389/tcp Tue, Sep 16, 2025 9:52 PM UTC
TCP timestamps 2.6 (Low) 80 % 10.10.1.16 general/tcp Tue, Sep 16, 2025 9:43 PM UTC
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 3 of 3
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net
Menu Parrot Terminal Greenbone Security Ass...


Applications Places System
Tue Sep 16, 18:00
Greenbone Security Assistant - Report Details - Mozilla Firefox
https://127.0.0.1:9392/report/6925bef9-8c8e-468b-bf94
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Report: Tue, Sep 16, 2025 9:40 PM UTC
Done
ID: 6925bef9-8c8e-468b-bf94-f5ef86cf530b
Created: Tue, Sep 16, 2025 9:41 PM UTC
Modified: Tue, Sep 16, 2025 9:58 PM UTC
Owner: admin
Information Results (3 of 47) Hosts (1 of 1) Ports (2 of 26) Applications (0 of 0) Operating Systems (1 of 1) CVEs (1 of 1) Closed CVEs (9 of 9) TLS Certificates (0 of 0) Error Messages (0 of 0) User Tags (0)
1 - 3 of 3
Vulnerability Severity QoD Host IP Name Location Created
DCE/RPC and MSRPC Services Enumeration Reporting 5.0 (Medium) 80 % 10.10.1.16 135/tcp Tue, Sep 16, 2025 9:53 PM UTC
Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
Detection Result
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:
Port: 1536/tcp
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net
Menu Parrot Terminal Greenbone Security Ass...

Module 03: Information Security Threats and Vulnerability Assessment – Lab Summary

This module demonstrated how attackers create and deploy malware and how defenders can assess system vulnerabilities.

In **Lab 1**, I explored Remote Access Trojans (Theef and njRAT). The Theef server executable was blocked by Windows Defender group policy, highlighting built-in OS protections. The njRAT client successfully launched but the remote shell was non-interactive, demonstrating RAT capabilities in a controlled environment without live execution.

In **Lab 2**, I used the JPS Virus Maker tool to generate a proof-of-concept virus, reinforcing how malicious code can be customized with disruptive payloads.

In **Lab 3**, I performed a vulnerability assessment using OpenVAS, which provided experience with scanning hosts, identifying vulnerabilities, and analyzing results through Greenbone Security Assistant.

Together, these labs reinforced key concepts of malware creation, propagation, and detection, as well as the importance of vulnerability management in protecting organizational systems.