

- C. Dictionary Attack
- D. Password Guessing

3. An attacker is cracking the password by trying every possible combination of alpha-numeric characters, which of the following types of Password Cracking is this?

- A. Brute Force Attack
- B. Default Password
- C. Dictionary Attack
- D. Password Guessing

4. Addition of characters in the password to make it one-way function is called:

- A. Password Encryption
- B. Password Hashing
- C. Password Padding
- D. Password Salting

5. Which of the following is a framework that can perform automated attacks on services, applications, ports & unpatched software?

- A. Wireshark
- B. Maltego
- C. Metasploit
- D. Syhunt Hybrid

6. Cracking password with pre-computed hashes is:

- A. Rainbow Table Attack
- B. Brute Force Attack
- C. Dictionary Attack
- D. Password Guessing

7. How can you mitigate a rainbow table attack?

- A. Changing Default Password
- B. Configuring Unpredictable Password
- C. Password Salting
- D. Password Hashing

## Chapter 7: Malware Threats

### Technology Brief

Malware is the abbreviation of the term Malicious Software. The term malware is an umbrella term that defines a wide variety of potentially harmful software. This malicious software is specially designed for gaining access to target machines, stealing information, and harming the target system. Any software designed with malicious intention that allows damaging, disabling, or limiting the control of the authorized owner and passing control of a target system to a malware developer or attacker, or allows any other malicious intent, can be considered malware. Malware can be classified into various types including Viruses, Worms, Keyloggers, Spywares, Trojans, Ransomware, and other malicious software. Malware is the most critically dangerous problem nowadays. Typical viruses and worms rely on older techniques whereas upcoming malwares are coded for infecting new technology, which makes them more dangerous.

## Malware Propagation Methods

There are different methods, through which malware can get into a system and infect it. Users should be careful while interacting with other devices and the internet. Some of the methods that are still popular for the propagation of malware are:

### ■ *Free Software*

When software is available on the internet for free, it often contains additional software and applications that may belong to the offering organization—bundled later by any third party to propagate this malicious software. The most common example of downloading free software is wrapping malicious software with a fake crack file of any popular and in-demand paid software for free. When users attempt to install this free crack, they end up infecting their systems. Usually, free software contains malicious software, or sometimes it only contains a malware.

### ■ *File Sharing Services*

File sharing services, such as torrent and peer-to-peer file sharing, transfer files from multiple computers. During transfer, a file can be infected. Similarly, any infected file may additionally transfer to other files because there may be a computer with low, or no security policies.

### ■ *Removable Media*

Malware can also propagate through removable media such as a USB. Various advanced removable media malware has been introduced that can propagate through the storage area of a USB as well as through firmware embedded in the hardware. Apart from a USB, external hard disks, CDs, and DVDs can also bring malware along with them.

### ■ *Email Communication*

In organizations, communicating through emails is very common. Malicious software can be sent through email attachments or via malicious URLs.

### ■ *Not using a Firewall or Anti-Virus*

Disabling security firewalls and anti-virus programs or not using internet security software can also allow malicious software to be downloaded on a system. Anti-viruses and internet security firewalls can block malicious software from downloading itself automatically and alert upon detection.

## The Trojan Concept

Trojan horse is a malicious program that misleads users about its actual intentions. This term derives from the Greek story of a great wooden horse. During their war against Troy, the Greeks fooled the Trojans into wheeling this horse into the city as a trophy. The horse had soldiers hiding inside it, waiting to enter the city. As night fell, the soldiers came out and attacked, destroying the whole city.

Like its namesake, Trojan misleads users about its actual intentions in order to avoid being detected while scanning and sandboxing, and waits for the best time to attack. Trojan may provide unauthorized access to an attacker, as well as access to personal information. Trojan can also lead to infection of other connected devices across a network.

## Trojan

Any Malicious Program misleading the user about its actual intention is classified as Trojan. Trojans are typically spread by Social Engineering.

The purpose or most common use of Trojan programs are:

- Creating a Backdoor
- Gaining Unauthorized Access
- Stealing Information
- Infecting Connected Devices
- Ransomware Attacks
- Using Victims for Spamming
- Using Victims as Botnet
- Downloading other Malicious Software
- Disabling Firewalls

Port Number Port Type

2 TCP

20 TCP

2 1 TCP

22 TCP

23 TCP

25 TCP

3 1 TCP

80 TCP

42 1 TCP

456 TCP

555 TCP

666 TCP 100 1 TCP 10 1 1 TCP 1095– 1098 TCP 1 170 TCP 1234

TCP 10000 TCP 10080 TCP 12345 TCP 17300 TCP

27374 TCP

65506 TCP

5300 1 TCP

65506 TCP

Trojans Death Senna Spy

Blade Runner / Doly Trojan / Fore / Invisible FTP / WebEx / WinCrash

Shaft  
Tiny Telnet Server

Antigen / Email Password Sender / Terminator / WinPC / WinSpy

Hackers Paradise / Masters Paradise

Executor

TCP Wappers Trojan

Hackers Paradise

Ini-Killer / Phase Zero / Stealth Spy

Satanz Backdoor

Silencer / WebEx

Doly Trojan

RAT

Psyber Stream Server / Voice

Ultors Trojan

Dumaru.Y

SubSeven 1.0– 1.8 / MyDoom.B

VooDoo Doll / NetBus 1.x, GabanBus, Pie Bill Gates, X-Bill NetBus

Kuang2 / SubSeven server (default for V2. 1-Defcon) SubSeven

Remote Windows Shutdown

Various names: PhatBot, Agobot, Gaobot

*Table 7-01: Known Ports used by Trojans*

## The Trojan Infection Process

The infection process using a Trojan is comprised of five steps. Following these steps an attacker can infect a target system.

1. Create a Trojan using Trojan Construction Kit.
2. Create a Dropper.
3. Create a Wrapper.
4. Propagate the Trojan.
5. Execute the Dropper.

## Trojan Construction Kit

The Trojan Construction Kit allows attackers to create their own Trojans. These customized Trojans can be more dangerous for the

target, as well as the attacker, if it backfires or is not executed properly. These customized Trojans, created with construction kits, can avoid detection from virus and Trojan scanning software. Some Trojan Construction Kits are:

- Dark Horse Trojan Virus Maker
- Senna Spy Generator
- Trojan Horse Construction Kit
- Progenic mail Trojan Construction Kit
- Pandora's Box

### *Droppers*

A Dropper is a software or program that is specially designed for delivering a payload on the target machine. The main purpose of a dropper is to install malware codes on to a victim's computer without alerting and while avoiding detection. It uses various methods to spread and install malware.

### *Trojan-Dropper Tools*

- TrojanDropper: Win32/Rotbrow.A
- TrojanDropper: Win32/Swisyn
- Trojan: Win32/Meredrop
- Troj/Destover-C

### *Wrappers*

These are non-malicious files that bind a malicious file to propagate the Trojan. Basically, a wrapper binds a malicious file in order to create and propagate the Trojan along with it to avoid detection. Wrappers are often popular executable files such as games, music, and video files, as well as any other non-malicious file.

### *Crypters*

A Crypter is software used while creating Trojans. The basic purpose of a Crypter is to encrypt, obfuscate, and manipulate the malware and malicious programs. Using a Crypter for hiding a malicious program

makes it even more difficult for security programs to detect malware. They are popularly used by hackers to create malware that is capable of bypassing security programs by presenting itself as a non-malicious program until it gets installed.

Some of the available Crypters for hiding malicious programs are:

- Cryogenic Crypter
- Heaven Crypter
- Swayz Cryptor

## Trojan Deployment

The Trojan deployment process is simple. An attacker uploads the Trojan to a server from where it can be downloaded immediately the victim clicks on the link. After uploading the Trojan to the server, the attacker sends an email containing a malicious link. When the victim receives this spam email, which may be offering something he/she is interested in, and clicks the link, it connects the system to the Trojan Server and downloads the Trojan to the victim's PC. Once installed, the Trojan connects the attacker to the victim by providing unauthorized access or extracts secret information, or performs any specific action desired by the attacker.

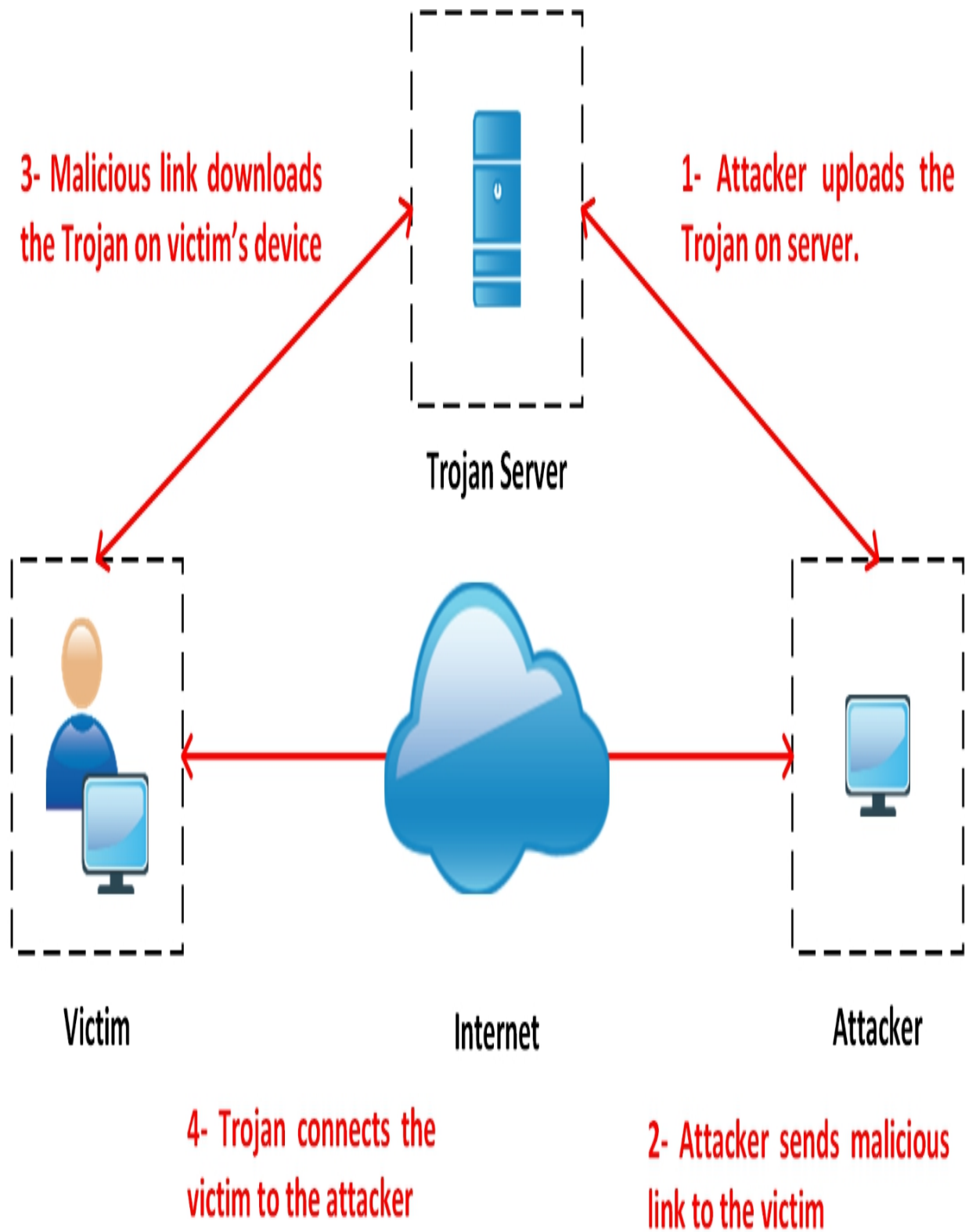


Figure 7-01: Linux Log Directory  
Types of Trojans



### ■ *Command Shell Trojans*

Command Shell Trojans are capable of providing remote control of a victim's command shell. Once the Trojan server of the command shell Trojan, such as Netcat, is installed on the target machine, it opens the port for a command shell connection to its client application installed on the attacker's machine. This Client-Server based Trojan provides access to the command line.

### ■ *Defacement Trojans*

Using Defacement Trojans, an attacker can view, edit, and extract information from any Windows program. By using this information, an attacker replaces strings, images, and logos often to leave their mark. They also use User-Styled Custom Application (UCA) to deface programs. Website defacement is well-recognized; it is similar to the concept of applications running on the target machine.

### ■ *HTTP/HTTPS Trojans*

HTTP and HTTPS Trojans bypass the firewall inspection and execute on the target machine. After execution, they create a HTTP/HTTPS tunnel to communicate with the attacker from the victim's machine.

### ■ *Botnet Trojans*

Botnets are the number of compromised systems (zombies). These compromised systems are not limited to any specific LAN; they may be spread over a large geographical area. These botnets are controlled by a Command and Control Center. These botnets are used to launch attacks such as Denial of Service, Spamming, etc.

### ■ *Proxy Server Trojans*

A Trojan-Proxy Server is a standalone malware application that is capable of turning the host system into a proxy server. Proxy Server Trojan allows an attacker to use the victim's computer as a proxy by enabling the proxy server on the victim's system. This technique is used to launch further attacks by hiding the actual source of the attack.

### ■ *Remote Access Trojans (RAT)*

Remote Access Trojan (RAT) allows an attacker to get remote desktop access to a victim's computer by enabling Port, which allows GUI

access to the remote system. RAT includes a backdoor for maintaining administrative access and control over the victim. Using RAT, an attacker can monitor a user's activity, access confidential information, take screenshots, and record audio and video using a webcam, format drives, and alter files, etc.

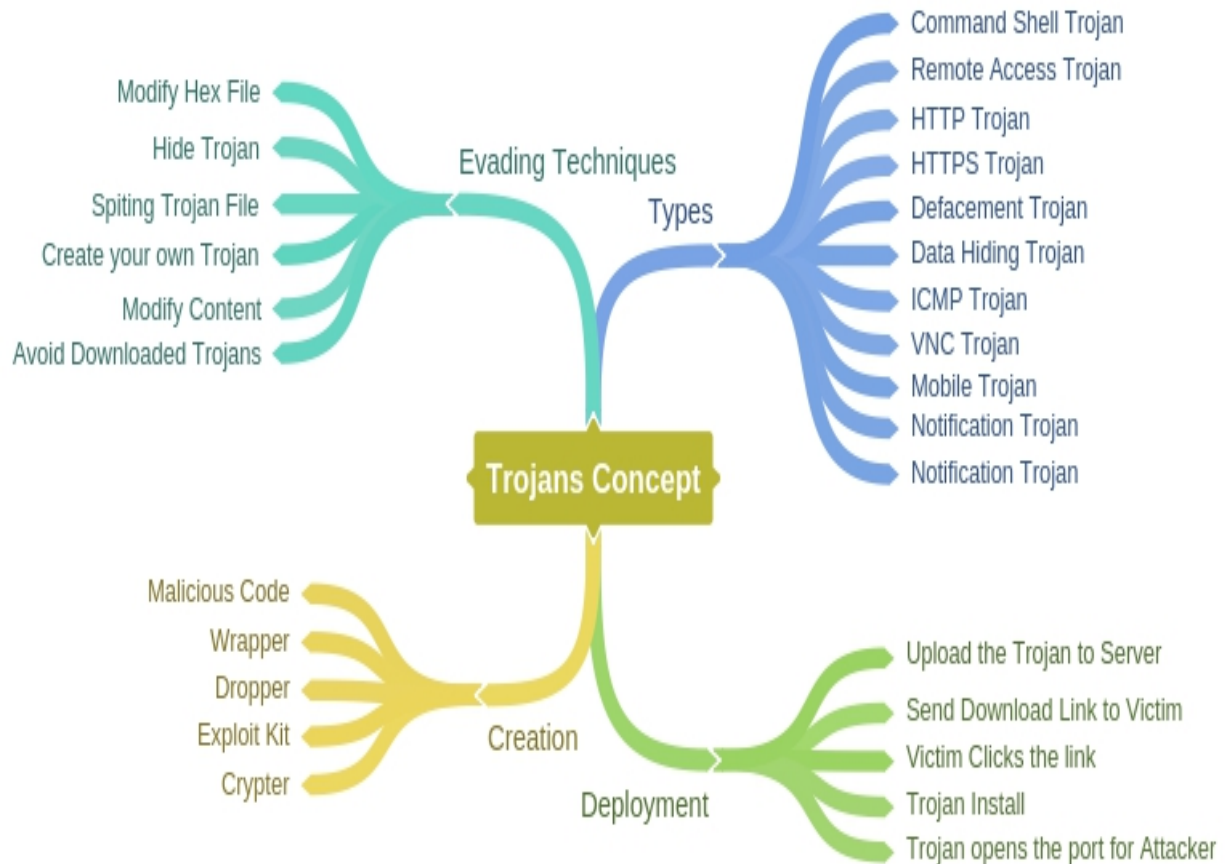
The following is a list of RAT tools:

- Optix Pro
- MoSucker
- BlackHole RAT
- SSH-R.A.T
- njRAT
- Xtreme RAT
- DarkComet RAT
- Pandora RAT
- HellSpy RAT
- ProRat
- Theef

Some other types of Trojans are:

- FTP Trojans
- VNC Trojans
- Mobile Trojans
- ICMP Trojans
- Covert Channel Trojans ■ Notification Trojan
- Data Hiding Trojan

Mind Map  
Trojan's



**Note:** A covert channel is a type of attack that creates the capability of transferring information objects between processes that the computer security policy prevents from communicating.

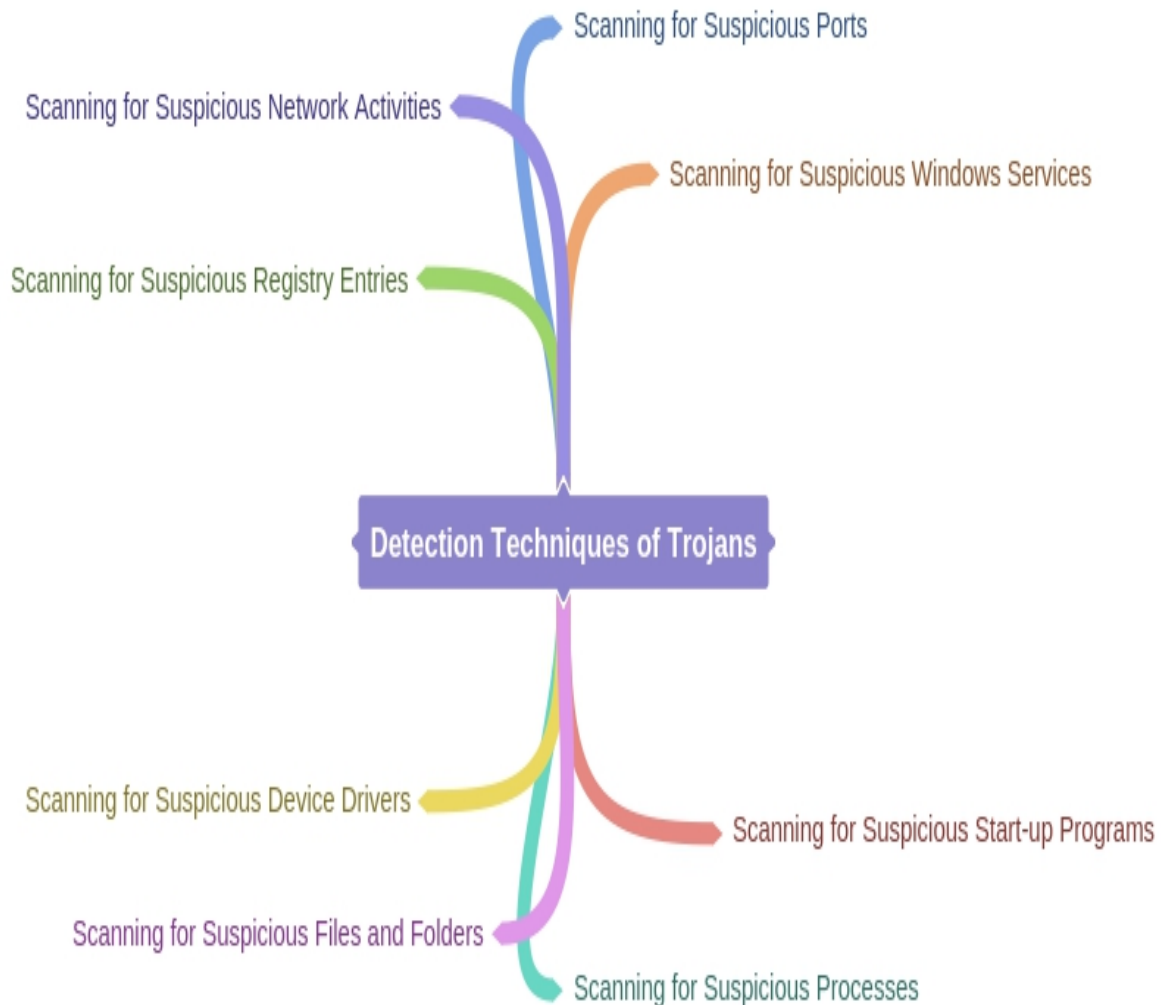
## Trojan Countermeasures

A network or a system can be protected by following the countermeasures for preventing Trojan attacks. Following are some key countermeasures that can be followed to prevent these attacks and protect your system.

- Avoid clicking on suspect email attachments
- Block unused ports
- Monitor network traffic
- Avoid downloading from untrusted sources
- Install updated security and anti-virus software
- Scan removable media before use

- Verify file integrity
- Enable auditing
- Install configured host-based firewall
- Install intrusion detection software

### *Detection Techniques for Trojans*



### Virus and Worm Concepts

Viruses are the oldest form of malicious programs; they were first introduced in 1970. In this section, we will discuss viruses and worms, how viruses are classified as different from other malicious programs, how to create viruses, and how viruses infect a target.

## Viruses

A Virus is a self-replicating program; it is capable of producing multiple copies of itself by attaching to another program of any format. These viruses can be executed just after being downloaded. They may either be configured to execute on a triggering event (wait for the host to execute them) or remain in sleep mode for a predetermined time before execution. The major characteristics of viruses are:

- Self-replicates
- Corrupts files and programs
- Infects other file and programs
- Alters data
- Transforms itself
- Encrypts itself

### *Stages of a Virus Life Cycle*

The process of developing a virus till its detection is divided into the following six stages. These stages include the creation of a virus program, its execution, detection, and antivirus stages. The methodology of developing a virus is classified as:

#### ■ Design

In the Design phase, a virus is created. To design a virus, the developer can create their own virus code completely from scratch by using programming languages or construction kits.

#### ■ Replication

In the Replication phase, when the virus is deployed, it replicates itself for a certain time period in the target system. After that period, it will spread itself. Replication of different viruses may differ depending upon how the developer wants to replicate them. Usually, this replication process is very fast and infects the target in a short period of time.

#### ■ Launch

The Launch stage is when a user accidentally launches the infected program. Once this virus is launched, it starts performing the actions it was designed for. For example, a virus may be specially designed for destroying data. Once the virus is activated, it starts corrupting data.

## ■ Detection

In the Detection phase, the behavior of a virus is observed and the virus is identified as a potential threat to a system. Typically, anti-virus developers observe the behavior of a reported virus.

## ■ Incorporation

Anti-virus software developers identify, detect, and observe the behavior of a virus and then design a defensive code or an update to provide support for an older version of anti-virus to detect this new type of virus.

## ■ Elimination

By installing the update of an anti-virus or downloading the newer version of antivirus capable of detecting advanced threats, a user can eliminate the threat from its Operating System.

## *Working of Viruses*

A Virus works in a two-phase process in which a virus replicates itself onto an executable file and attacks on a system. Different phases are defined below:

### *1. Infection Phase*

During the Infection phase, the virus planted on a target system replicates itself onto an executable file. By replicating into legitimate software, it can be launched when a user runs the authentic application. These viruses spread by reproducing and infecting the programs, documents, or email attachments. Similarly, they can be propagated through emails, file sharing, or files downloaded from the

internet. They can enter into an Operating System through CDs, DVDs, USB-drives and any other sort of digital media.

## *2. Attack Phase*

In the Attack phase, the infected file is executed either intentionally by an intruder or accidentally by a user. Viruses normally require a triggering action to infect a victim. This infection can completely destroy the system or may corrupt the program files and data. Some viruses can initiate an attack when they are executed, but they can also be configured to infect according to certain pre-defined conditions.

### **Note:**

**Multipartite Virus:** A multipartite virus infects and spreads in multiple ways. This term is used to define the first viruses including DOS executable files and PC BIOS boot sector virus code.

**Macro Virus:** A macro virus is a computer virus written in the same macro language used for software programs, including Microsoft Excel and Microsoft Word. When a macro virus infects a software application, it causes a sequence of actions to begin automatically when the application is opened.

**Polymeric Virus :** A polymorphic virus is a complicated computer virus that affects data types and functions. It is a self-encrypted virus designed to avoid detection by a scanner. Upon infection, the polymorphic virus duplicates itself by creating usable, albeit slightly modified, copies of itself.

**Stealth Virus:** A stealth virus is a computer virus that uses various mechanisms to avoid detection by antivirus software. Generally, stealth defines any approach to doing something while avoiding notice.

## **Ransomware**

Ransomware is a malware program that restricts the access to system files and folders by encrypting them. Some types of ransomware may

lock the system as well. Once the system is encrypted, it requires a decryption key to unlock it and its files. An attacker then demands a ransom payment before providing the decryption key to remove restrictions. Online payments using digital currencies that are difficult to trace like Ukash and Bitcoin are used for ransoms. Ransomware is normally deployed using Trojans. One of the best examples of ransomware is the WannaCry Ransomware attack. Following are the most common and widely known types of ransomware:

- Cryptobit Ransomware
- CryptoLocker Ransomware
- CryptoDefense Ransomware
- CryptoWall Ransomware
- Police-themed Ransomware

*Examples of Ransomware:*

- Crypto-Locker

*Crypto-Malware:*

This encrypts all the data or files either permanently or temporarily. It is more intended for denial of service by permanently encrypting files or doing so temporarily until a ransom is paid.

*How to prevent this infection?*

- Update the Operating System and applications
- Backup all data offline
- Install anti-virus and update the anti-virus signature

*Types of Viruses*

- System or Boot Sector Viruses

A Boot Sector Virus is designed to move Master Boot Record (MBR) from its actual location. A Boot Sector Virus responds from the original location of the MBR when the system boots – it executes the virus first. A boot sector virus alters the boot sequence by infecting the MBR. It infects the system causing boot problems, performance issues, instability, and inability to locate directories.



## ■ File and Multipartite Viruses

File or Multipartite Viruses infect systems in various ways. File viruses infect the files that are executable such as BAT files. A multipartite virus can infect the boot sector and files simultaneously – hence the term multipartite. Attack targets may include boot sector and executable files on the hard drive.

## ■ Macro Viruses

A Macro Virus is a type of virus that is specially designed for the applications of Microsoft Word, Excel, and other applications using Visual Basic for Application (VBA). Macro languages help to automate and create a new process, which is used abusively by running on a victim's system.

## ■ Cluster Viruses

Cluster viruses are designed for the dedicated use of attacking and modifying the file location table or directory table. Cluster viruses attacks in a different way. The actual file located in the directory table is altered so that file entries point to the infected file instead of an actual file. In this way, when a user attempts to run an application, the virus is executed instead.

## ■ Stealth/Tunneling Viruses

These types of viruses use different techniques to avoid being detected by an antivirus program. In order to evade detection, a stealth virus employs a tunnel technique to launch under the anti-virus via a tunnel, and intercepts requests from the Operating System interruption handler. Anti-viruses use their own tunnels to detect these types of attacks.

## ■ Logic Bombs

A Logic Bomb virus is designed to remain in a waiting state or sleep mode until the end of a pre-determined period or an event or action occurs. When the condition is met, it triggers the virus to exploit and

perform the intended task. These logic bombs are difficult to detect, as they are unable to be detected in sleep mode and once they are detected it is too late.

## ■ Encryption Virus

Encryption Viruses are those viruses that use encryption and are capable of scrambling to avoid detection. Because of this, these viruses are difficult to detect. They use new encryption to encrypt and decrypt the code as it replicates and infects.

### *Other types of viruses*

Some other types of viruses are:

- Metamorphic Viruses
- File Overwriting or Cavity Viruses
- Sparse Infector Viruses
- Companion/Camouflage Viruses
- Shell Viruses
- File Extension Viruses
- Add-on and Intrusive Viruses
- Transient and Terminate and Stay Resident Viruses

### *Writing a Simple Virus Program*

Creating a virus is a simple process. However, it depends upon the intention of the developer. A high profile developer may prefer to design code from scratch. Following are some steps to creating a basic virus that can perform a certain action upon being

triggered. To create a virus, you need to have a Notepad application and Bat2com application. You can also create a virus using GUI-based applications.

### Simple Virus Program Using Notepad

1. Create a directory with a bat file and text file.
2. Open the Notepad application.
3. Enter the code as shown:

```
@echo off  
for %%f in (*.bat) do copy %%f + Virus.bat
```

```
Del c:\Windows\*.*
```

4. Save the file in .bat format.

5. Convert the file using the bat2com utility or bat to the .exe converter.

6. This will save an Exe file in the current directory, which will execute upon clicking. *Virus Generating Tools*

- Sam's Virus Generator
- JPS Virus Maker
- Andreinick05's Batch Virus Maker
- DeadLine's Virus Maker
- Sonic Bat – Batch File Virus Creator
- Poison Virus Maker



## Computer Worms

Worms are another type of malware. Viruses require a triggering event to execute, whereas worms can replicate themselves. Worms cannot attach themselves to other programs. A worm can propagate using File

transport and spread across the infected network, of which a virus is not capable.

*Examples of Worms:*

- Sobig Worm of 2003
- SQL Slammer Worm of 2003
- 2001 Attacks of Code Red and Nimba
- 2005 Zotob Worm

## Virus Analysis and Detection Methods

The Detection phase of a virus initiates with scanning. Initially, the suspected file is scanned for the signature string. In the second step of the detection method, the entire disk is checked for integrity. An integrity checker records the integrity of all files on a disk, usually by calculating the Checksum. If a file is altered by a virus, it can be detected through an integrity check. In an interception step, requests from the Operating System are monitored. Interception software is used to detect virus-resembling behaviors and to generate a warning for users. Code Emulation and Heuristic Analysis include behavioral analysis and code analysis of a virus by executing it in a sophisticated environment.

## Malware Reverse Engineering Sheep Dipping

Sheep Dipping is the analysis of a suspect file and packets against viruses and malware before allowing them to be available for users in an isolated environment. This analysis is performed on a dedicated computer. This initial line of defense runs with highly secure computing along with port monitoring, file monitoring, anti-viruses, and other security programs.

## Malware Analysis

Malware Analysis is the process of identifying a malware and ensuring that the malware is completely removed. This process includes observing the behavior of malware, scoping the potential threat to a

system and finding other measures. Before explaining the malware analysis, the need for malware analysis and the goal to be achieved by this analytics must be defined. Security analysts and security professionals at some point in their careers have all performed malware analysis. The major goal of malware analysis is to gain detailed information and observe the behavior of malware, to maintain incident response, and to take defensive actions to secure the organization.

The malware analysis process starts with preparing the Testbed for analysis. Security professionals get a virtual machine ready as a host Operating System where dynamic malware analysis will be performed by executing the malware over the guest Operating System. This host OS is isolated from other networks to observe the behavior of the malware by isolating it from the network.

After executing a malware in a Testbed, Static and Dynamic Malware analysis is performed. A network connection is also set up later to observe the behavior by using process monitoring tools, packet monitoring tools, and debugging tools like OllyDbg and ProcDump.

### *Goals of Malware Analysis*

Malware analysis goals are defined below:

- Diagnostics of threat severity or level of attack
- Diagnostics of the type of malware
- Scope the attack's impact
- Built defense to secure organization's network and systems
- Find a root cause
- Built incident response actions
- Develop anti-malware

### *Types of Malware Analysis*

Malware analysis is classified into two basic types:

- **Static Analysis**

Static Analysis or Code Analysis is performed by fragmenting the resources of the binary file without executing it and studying each

component. A disassembler such as IDA is used to disassemble the binary file.

- **Dynamic Analysis**

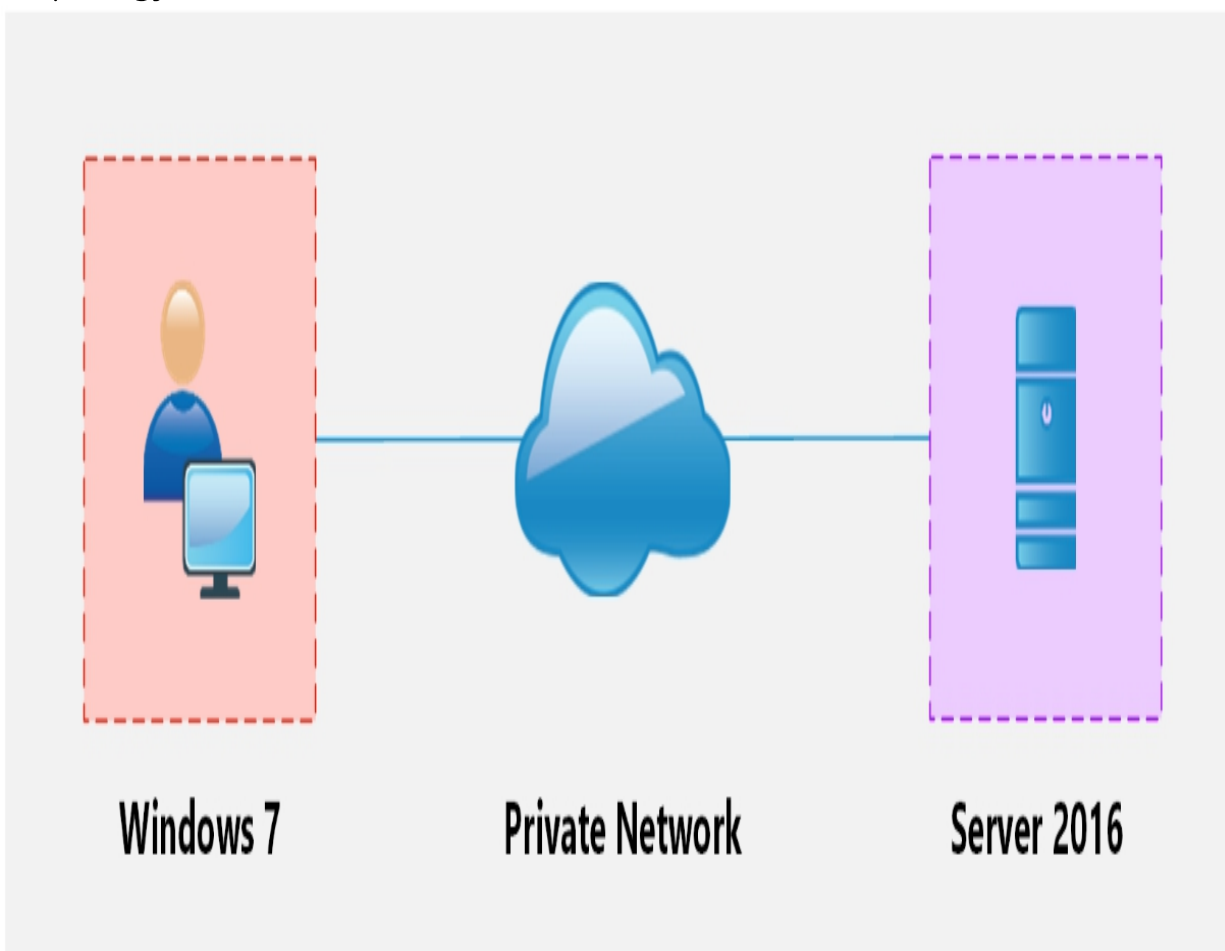
Dynamic Analysis or Behavioral Analysis is performed by executing the malware on a host and observing its behavior. These behavioral analyses are performed in a Sandbox environment.

Sandboxing technology helps in detecting threats in a dedicated manner in a sophisticated environment. During Sandboxing, malware is searched in the intelligence database for the analysis report. It might be possible that diagnostics details are available if the threat was previously detected. When a threat is diagnosed, its analytics are recorded for future use. If it is found that a match exists in a database, it helps in responding quickly.

## **Lab 7– 1: HTTP RAT Trojan**

**Case Study:** Using HTTP RAT Trojan, we are going to create an HTTP Remote Access Trojan (RAT) server on a Windows 7 machine (10. 10.50.202). When a Trojan file is executed on the remote machine (in our case, Windows Server 20 16 with the IP address 10. 10.50.2 1 1), it will create remote access of Windows Server 20 16 on Windows 7.

Topology:



*Figure 7-02: Topology Diagram*

Configuration and Procedure:

Go to a Windows 7 machine and run the HTTP RAT Trojan.

1. Uncheck "send notification with IP address to mail".
2. Configure Port.
3. Click "Create".



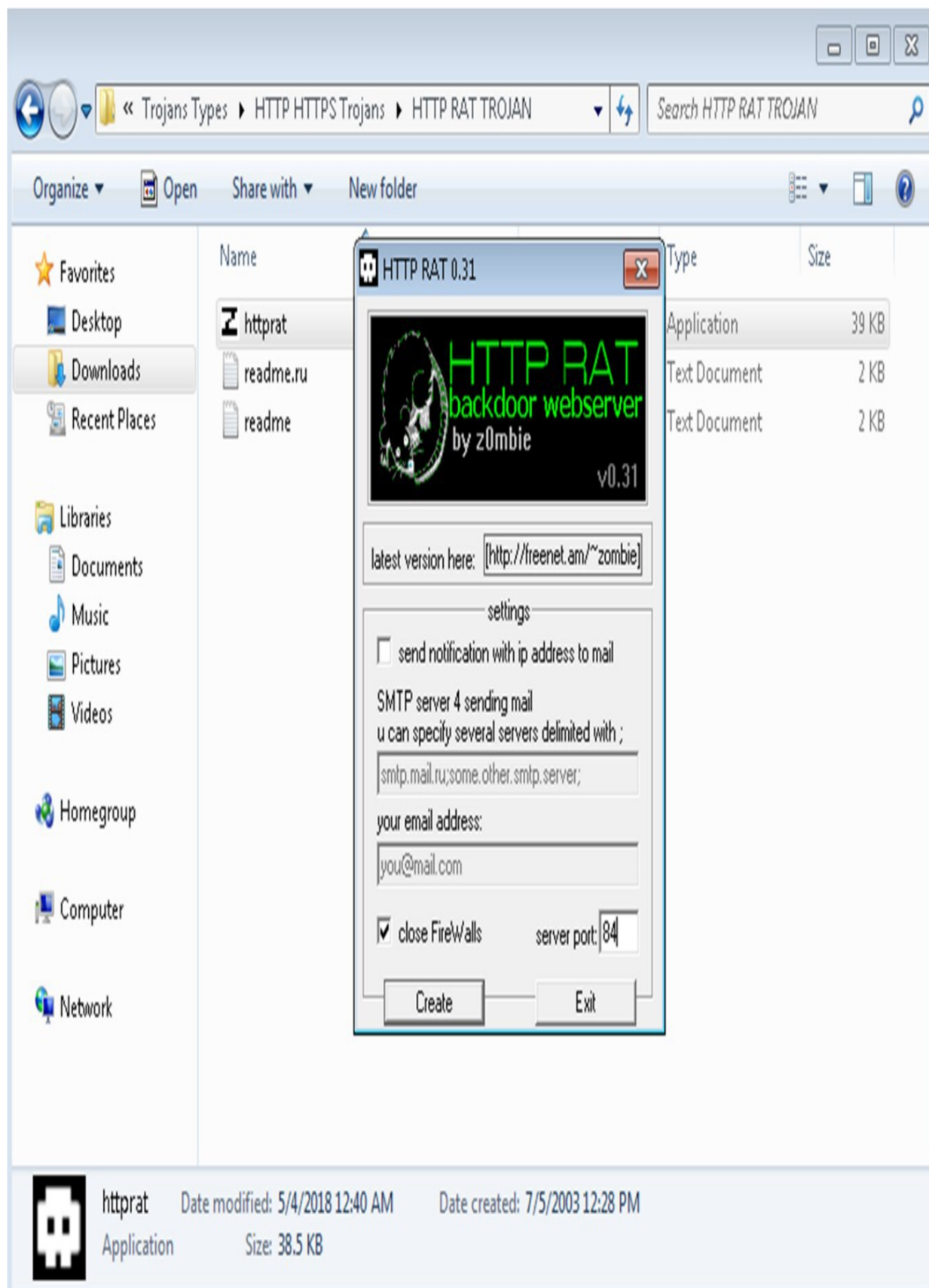
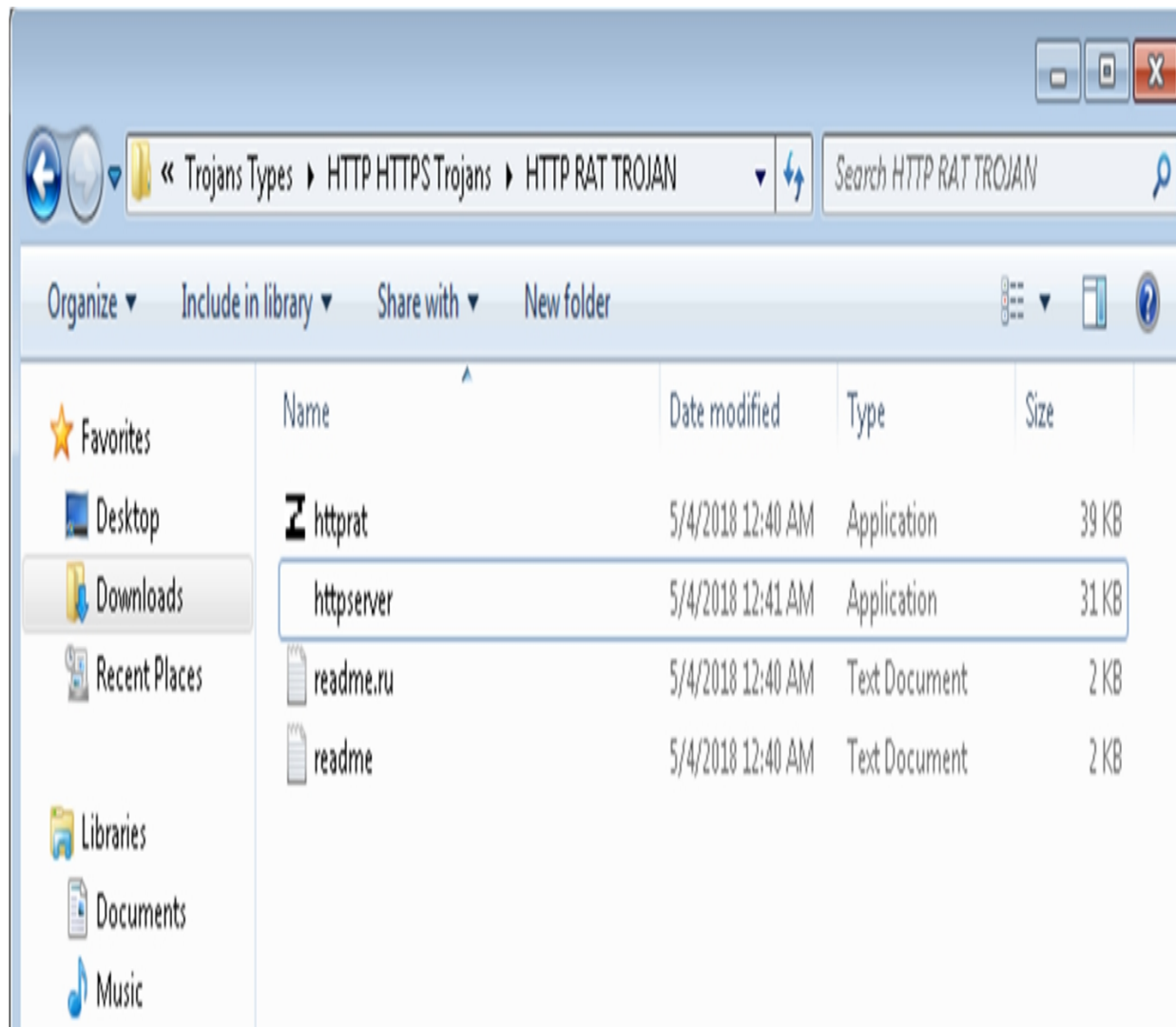


Figure 7-22: HTTP RAT Trojan

*Figure 7-03: HTTP RAT Trojan*

In the default directory where the application is installed, you will see a new executable file. Forward this file to the victim's machine.



*Figure 7-04: Trojan EXE File Created*

4. Log in to the victim's machine (in our case, Windows Server 20 16) and run the file.
5. Check the task manager for a running process; you will see an HTTP Server task is in process.

Task Manager

File Options View

Processes Performance Users Details Services

Name	8% CPU	30% Memory
Apps (1)		
> Task Manager	0%	7.4 MB
Background processes (20)		
> Antimalware Service Executable	0%	57.9 MB
Application Frame Host	0%	2.7 MB
> Global Network Inventory Servi...	0%	1.5 MB
Google Crash Handler	0%	0.3 MB
Google Crash Handler (32 bit)	0%	0.4 MB
Host Process for Windows Tasks	0%	3.6 MB
httpserver (32 bit)	0%	1.8 MB
> Microsoft Distributed Transacti...	0%	2.1 MB
RDP Clipboard Monitor	0%	2.3 MB
RDP Session Input Handler	0%	1.0 MB
Runtime Broker	0%	6.9 MB

^ Fewer details

End task


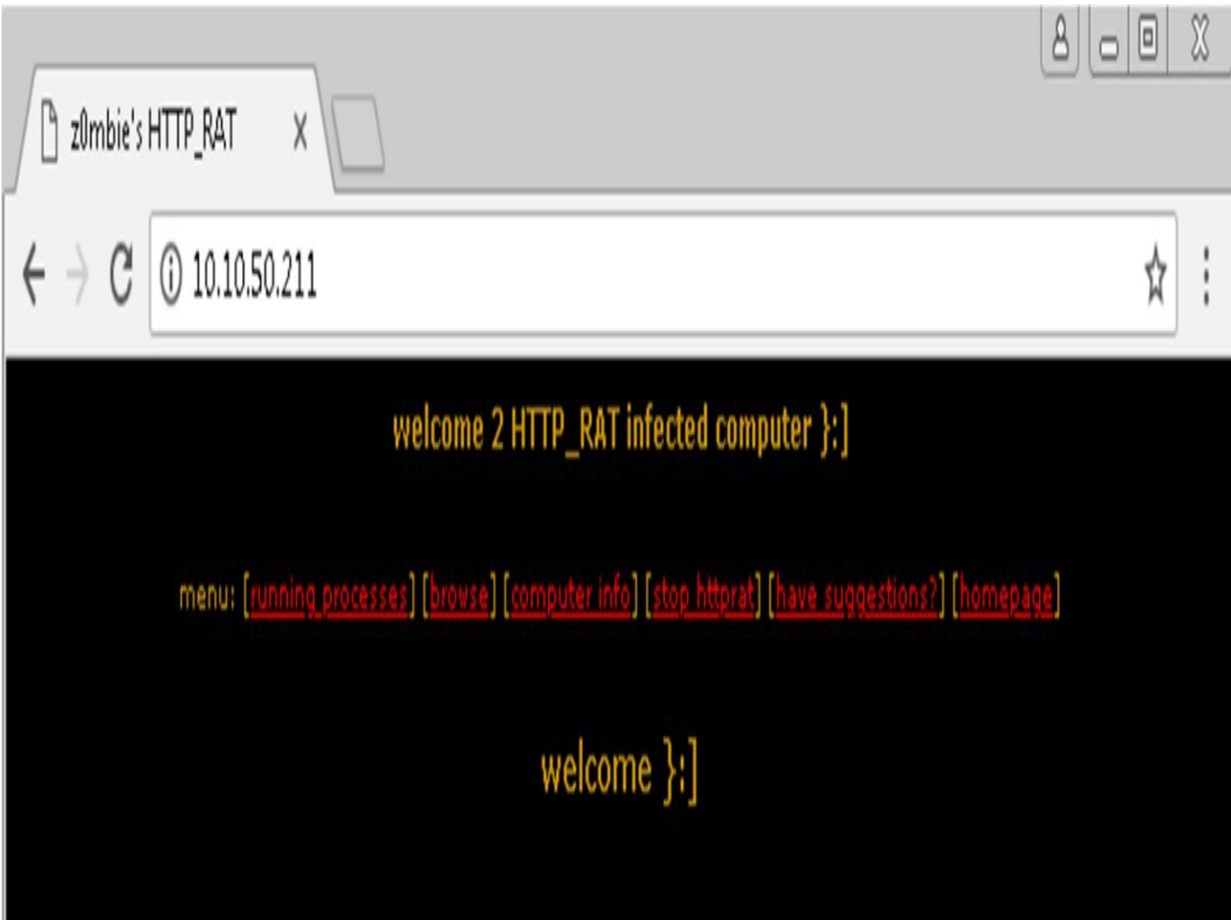


Figure 7-25: Trojan Process on the Victim Machine

*Figure 7-05: Trojan Process on the victim machine*

6. Go back to Windows 7.
7. Open a Web browser.
8. Go to the IP address of the victim's machine; in our case, 10.10.50.211.



*Figure 7-06: Accessing the Victim Using HTTP*

The HTTP connection is open from the victim's machine. You can check running processes and browse drives. You can also check the computer information of the victim by using this tool.

9. Click "Running Processes".

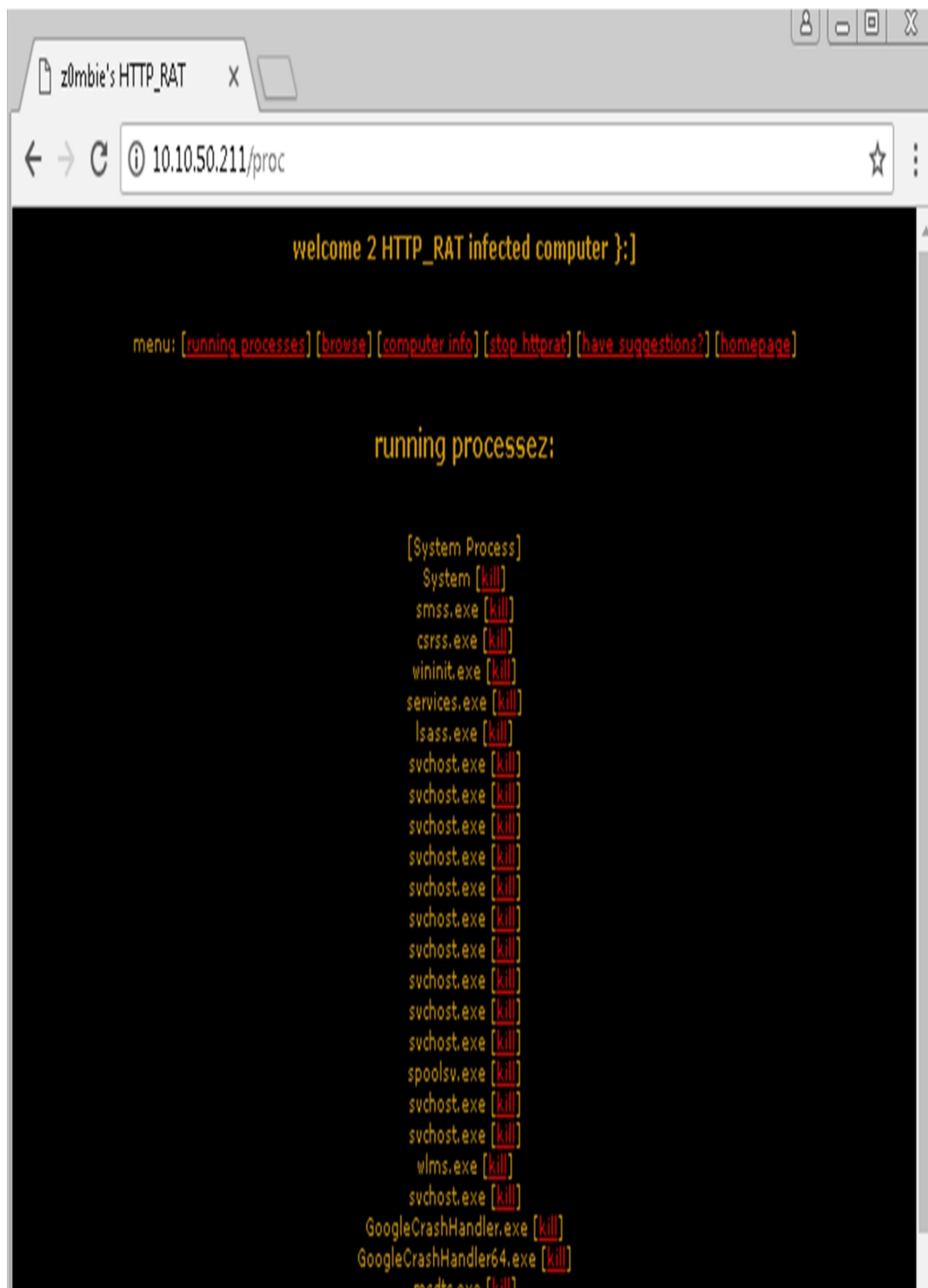


Figure 7-27: Running the Processes on the Victim

*Figure 7-07: Running the Process on the Victim*

Above output “running process” of victim’s machine is shown.

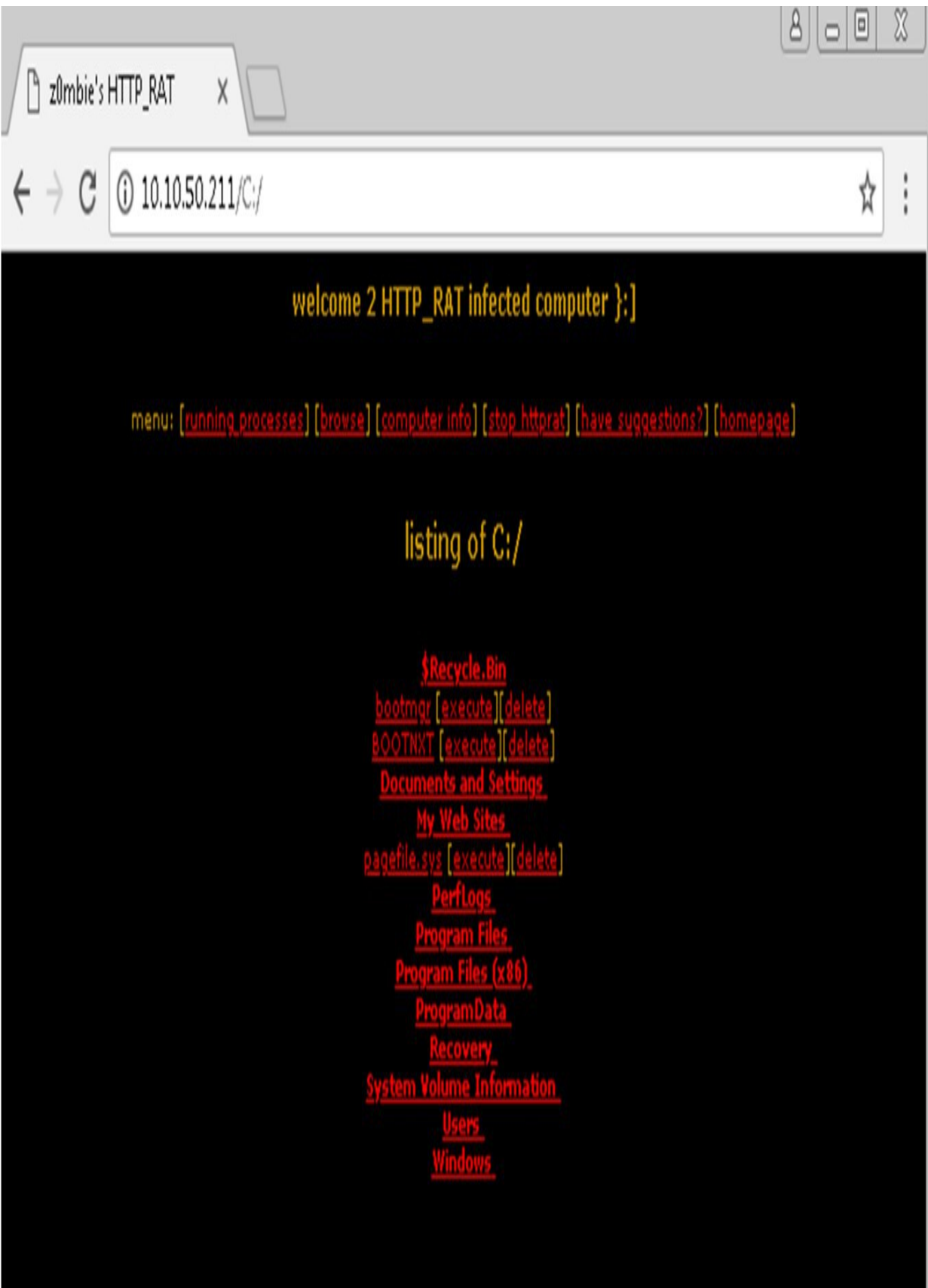
10. Click “Browse”.



*Figure 7-08: Browse Drives of the Victim*

The output shows drives.

11. Click “Drive C”.

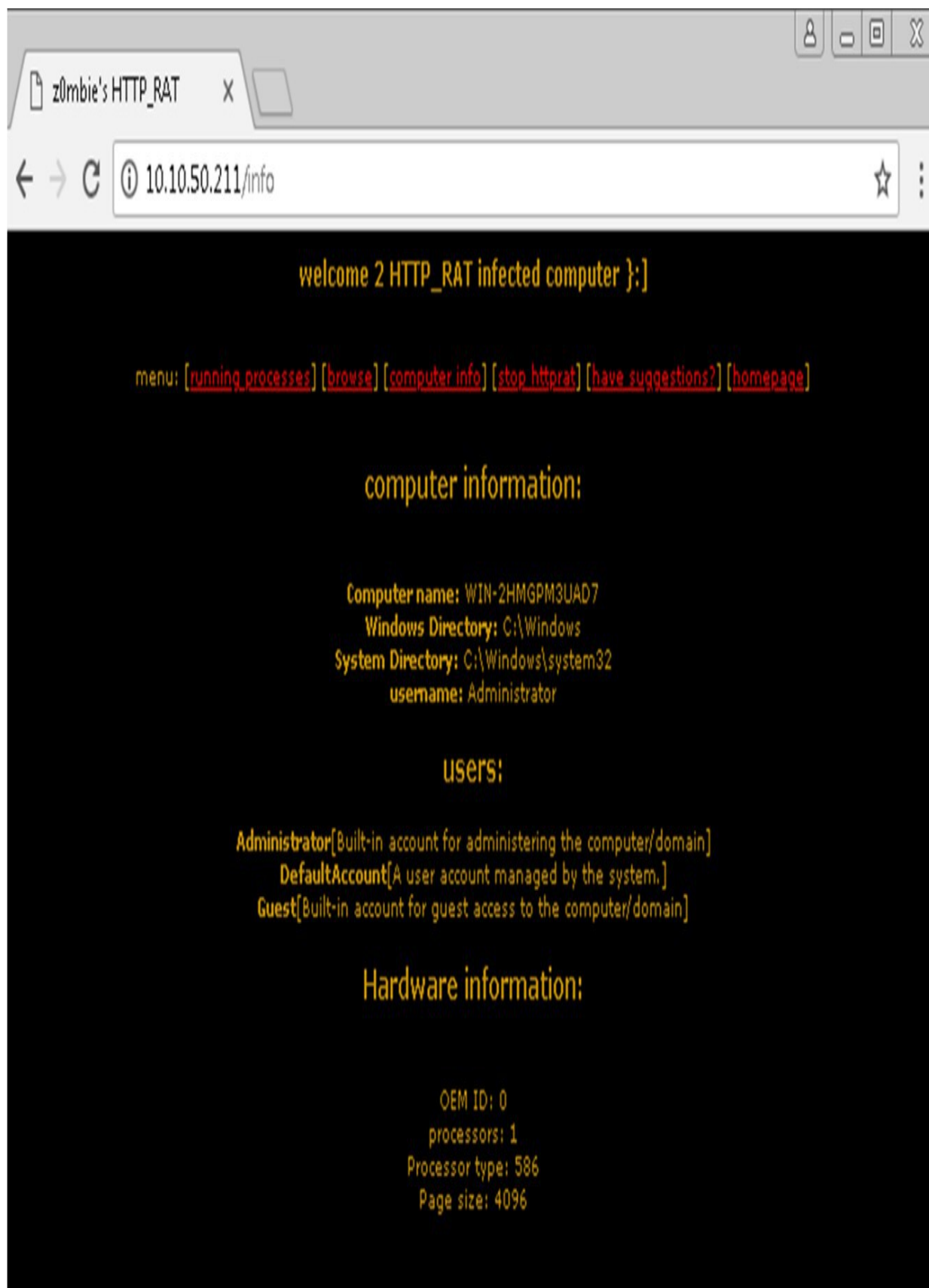




*Figure 7-09: C Drive of the Victim*

Output showing C drive.

12. Click “Computer Information”.



*Figure 7–10: Computer's Information of the Victim*

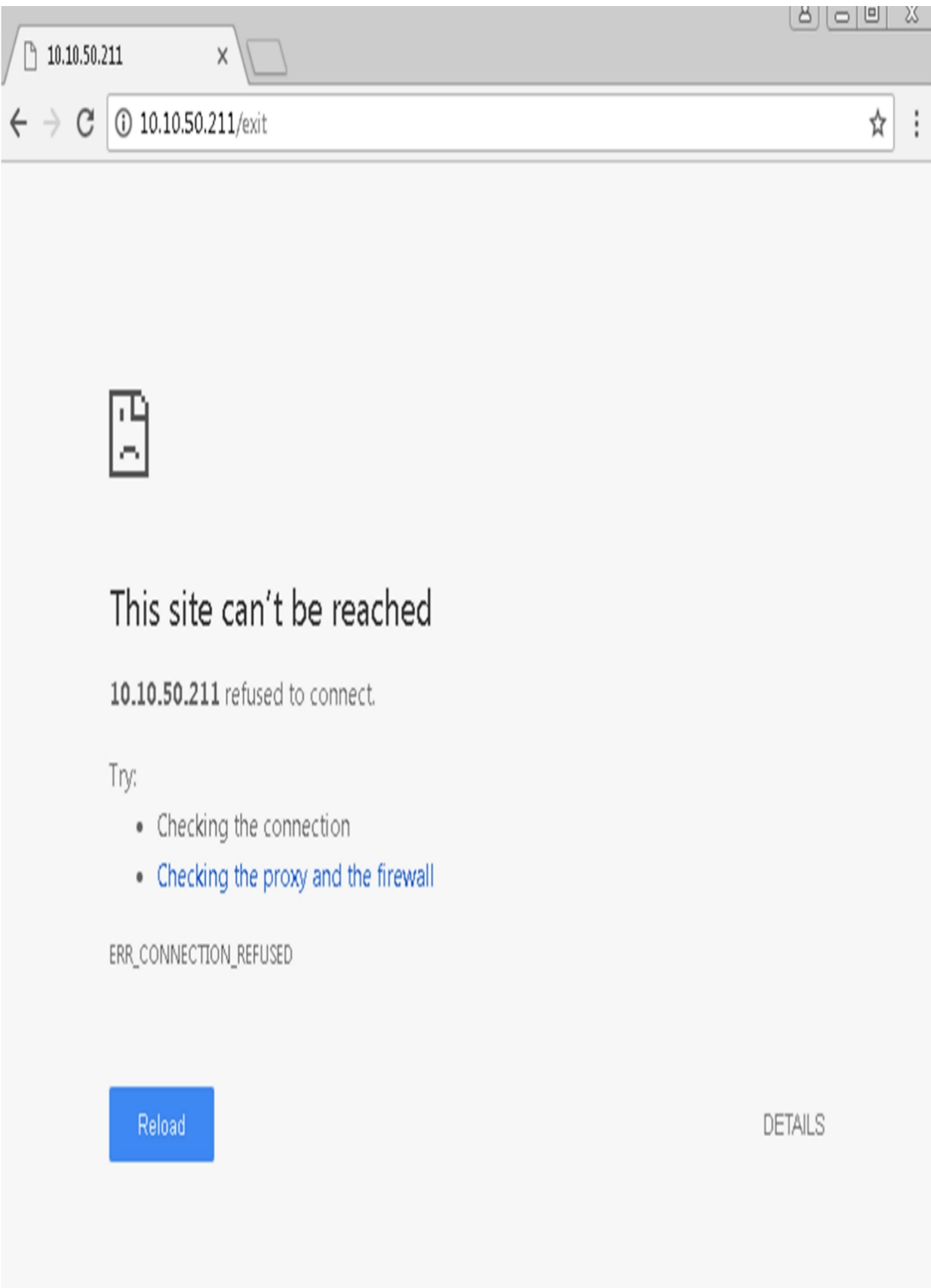
The output is showing computer information.

13. To terminate the connection, click “Stop\_httpRat”.



*Figure 7–11: Stop HTTP Connection*


14. Refresh the browser.




*Figure 7-12: Connection Terminated*

The connection is successfully terminated.


15. Go to Windows Server 2016 and check the running processes.



Recycle B



Google Chrome



httpserve

Task Manager

File Options View

Processes Performance Users Details Services

Name	2% CPU	29% Memory
Apps (1)		
Task Manager	0%	7.3 MB
Background processes (19)		
Antimalware Service Executable	0%	57.9 MB
Application Frame Host	0%	2.7 MB
Global Network Inventory Servi...	0%	1.4 MB
Google Crash Handler	0%	0.3 MB
Google Crash Handler (32 bit)	0%	0.4 MB
Host Process for Windows Tasks	0%	3.6 MB
Microsoft Distributed Transacti...	0%	2.1 MB
RDP Clipboard Monitor	0%	2.3 MB
RDP Session Input Handler	0%	1.0 MB
Runtime Broker	0%	6.8 MB
Search	0%	53.8 MB

^ Fewer details

End task

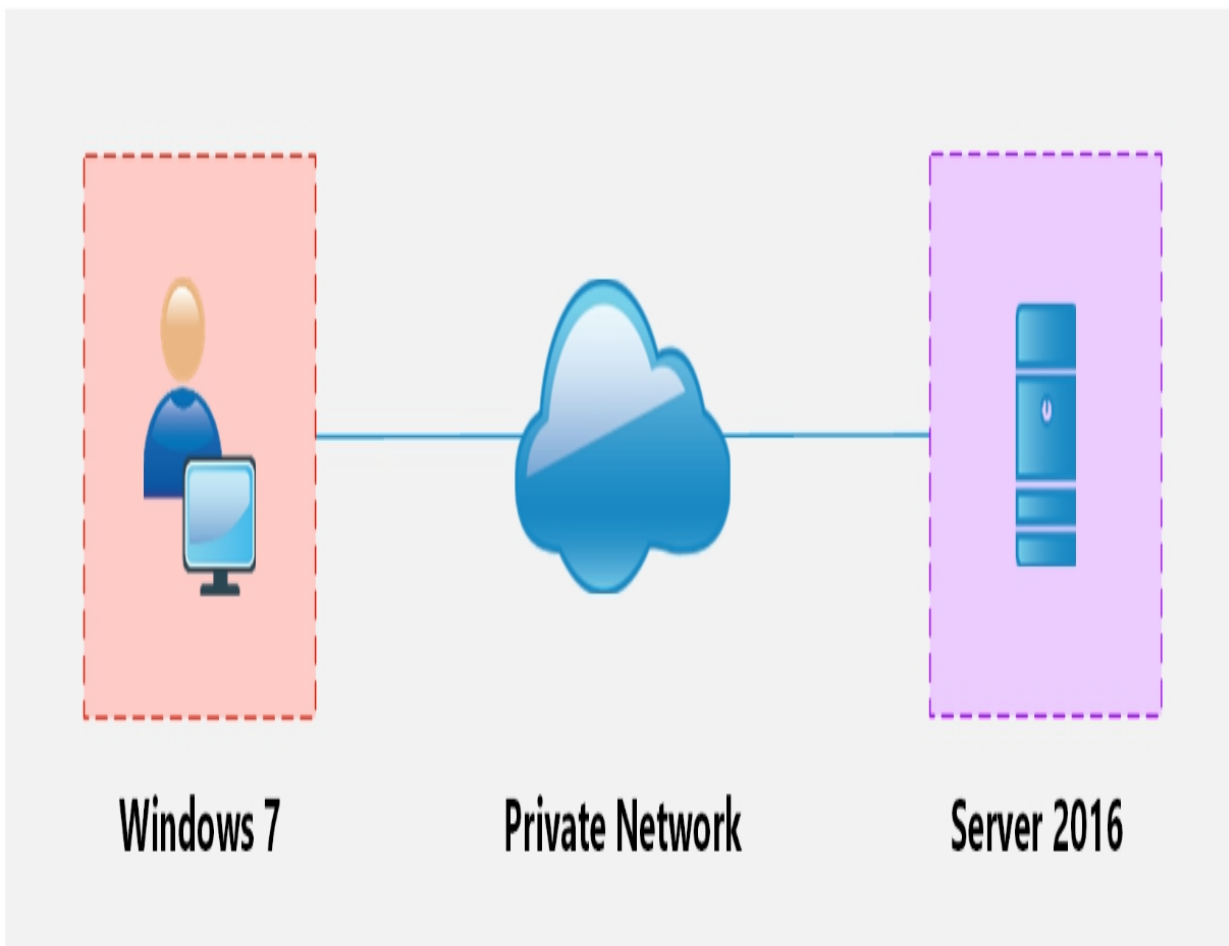
*Figure 7–13: Verifying Process*

The HTTP server process is terminated.

### Lab 7–2: Monitoring a TCP/IP Connection Using CurrPort Tool

**Case Study:** Implementing the previous lab, we are going to re-execute the HTTP Remote Access Trojan (RAT) on a Windows 12 machine ( 10. 10.50.2 1 1) and observe the TCP/IP connections to detect and kill the connection.

**Topology:**



*Figure 7–14: Topology Diagram*

**Configuration:**

1. Run the application Currports on Windows Server 20 16 and observe the processes.

CurrPorts							
File Edit View Options Help							
Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
lsass.exe	528	TCP	49670		0.0.0.0		
lsass.exe	528	TCP	49670		::		
services.exe	516	TCP	49669		0.0.0.0		
services.exe	516	TCP	49669		::		
snmptrap.exe	2200	UDP	162	snmptrap	0.0.0.0		
snmptrap.exe	2200	UDP	162	snmptrap	::		
spoolsv.exe	1472	TCP	49667		0.0.0.0		
spoolsv.exe	1472	TCP	49667		::		
svchost.exe	636	TCP	135	epmap	0.0.0.0		
svchost.exe	804	TCP	3389	ms-wbt-...	0.0.0.0		
svchost.exe	864	TCP	49665		0.0.0.0		
svchost.exe	980	TCP	49666		0.0.0.0		
svchost.exe	4128	TCP	49791		0.0.0.0		
svchost.exe	992	UDP	123	ntp	0.0.0.0		
svchost.exe	980	UDP	500	isakmp	0.0.0.0		
svchost.exe	2192	UDP	1900	ssdp	10.10.50.211		
svchost.exe	2192	UDP	1900	ssdp	127.0.0.1		
51 Total Ports, No Remote Connections, 1 Selected						NirSoft Freeware. <a href="http://www.nirsoft.n">http://www.nirsoft.n</a>	

Figure 7–15: Currports Application Showing Running Processes



2. Run the HTTP Trojan created in the previous lab.

CurrPorts

File
Edit
View
Options
Help

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
httpserver.exe	2644	TCP	80	http	0.0.0.0		
lsass.exe	528	TCP	49670		0.0.0.0		
lsass.exe	528	TCP	49670		::		
services.exe	516	TCP	49669		0.0.0.0		
services.exe	516	TCP	49669		::		
snmptrap.exe	2200	UDP	162	snmptrap	0.0.0.0		
snmptrap.exe	2200	UDP	162	snmptrap	::		
spoolsv.exe	1472	TCP	49667		0.0.0.0		
spoolsv.exe	1472	TCP	49667		::		
svchost.exe	636	TCP	135	epmap	0.0.0.0		
svchost.exe	804	TCP	3389	ms-wbt-...	0.0.0.0		
svchost.exe	864	TCP	49665		0.0.0.0		
svchost.exe	980	TCP	49666		0.0.0.0		
svchost.exe	4128	TCP	49791		0.0.0.0		
svchost.exe	992	UDP	123	ntp	0.0.0.0		
svchost.exe	980	UDP	500	isakmp	0.0.0.0		
svchost.exe	2192	UDP	1900	ssdp	10.10.50.211		

12 Total Ports, No Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

### *Figure 7–16: Trojan Connection*

The new process is added to the list.

You can observe the process name, protocol, local and remote port, and IP address information.

3. For more details, right click on “httpserver.exe” and go to “Properties”.

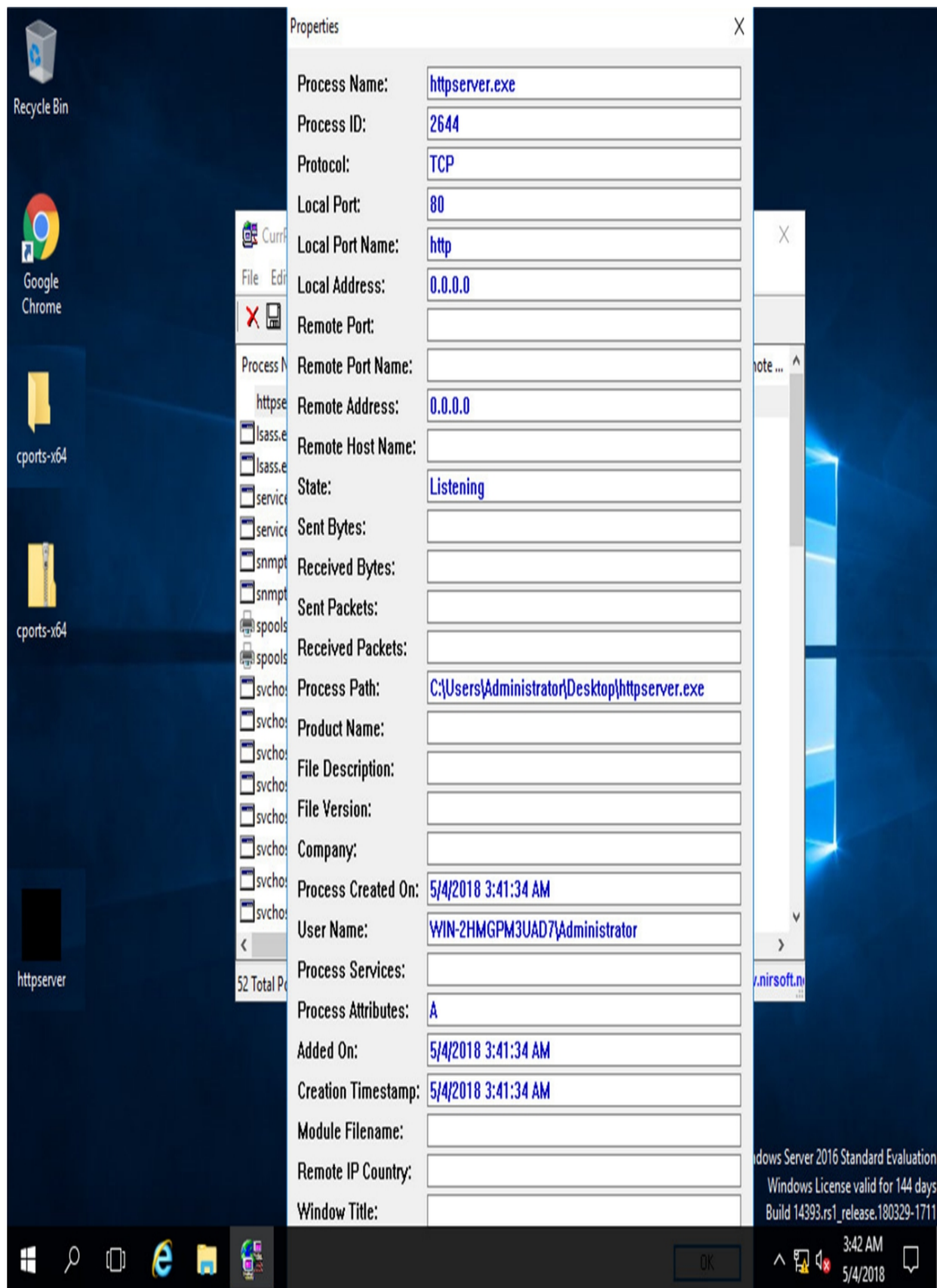


Figure 7-17: TCP Connection Properties

*Figure 7-17: TCP Connection Properties*

Properties shows more details about the TCP connection.

4. Go to a Windows 7 machine and initiate the connection as mentioned in the previous lab using a web browser.



*Figure 7-18: HTTP RAT Connection*

The connection is successfully established.

5. Go back to the Windows Server 2016. Kill the connection.



CurrPorts

File Edit View Options Help

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
httpserver.exe	264	TCP	80	...	...	...	...
lsass.exe	52	...	...	...	...	...	...
lsass.exe	52	...	...	...	...	...	...
services.exe	51	...	...	...	...	...	...
services.exe	51	...	...	...	...	...	...
snmptrap.exe	22	...	...	...	...	...	...
snmptrap.exe	22	...	...	...	...	...	...
spoolsv.exe	14	...	...	...	...	...	...
spoolsv.exe	14	...	...	...	...	...	...
svchost.exe	63	...	...	...	...	...	...
svchost.exe	80	...	...	...	...	...	...
svchost.exe	86	...	...	...	...	...	...
svchost.exe	98	...	...	...	...	...	...
svchost.exe	41	...	...	...	...	...	...
svchost.exe	99	...	...	...	...	...	...
svchost.exe	98	...	...	...	...	...	...
svchost.exe	21	...	...	...	...	...	...

57 Total Ports, No Remot...

IPNetInfo Ctrl+I

Close Selected TCP Connections Ctrl+T

Kill Processes Of Selected Ports

Include In Filter >

Exclude In Filter >

Clear All Filters F8

Save Selected Items Ctrl+S

Copy Selected Items Ctrl+C

Copy Remote IP Address F2

HTML Report - All Items

HTML Report - Selected Items

Choose Columns

Auto Size Columns Ctrl+Plus

Process Properties Ctrl+P

Properties Alt+Enter

Refresh F5

Freeware. <http://www.nirsoft.net>

Windows Server 2016 Standard Evaluation  
Windows License valid for 144 days  
Build 14393.rs1\_release.180329-1711



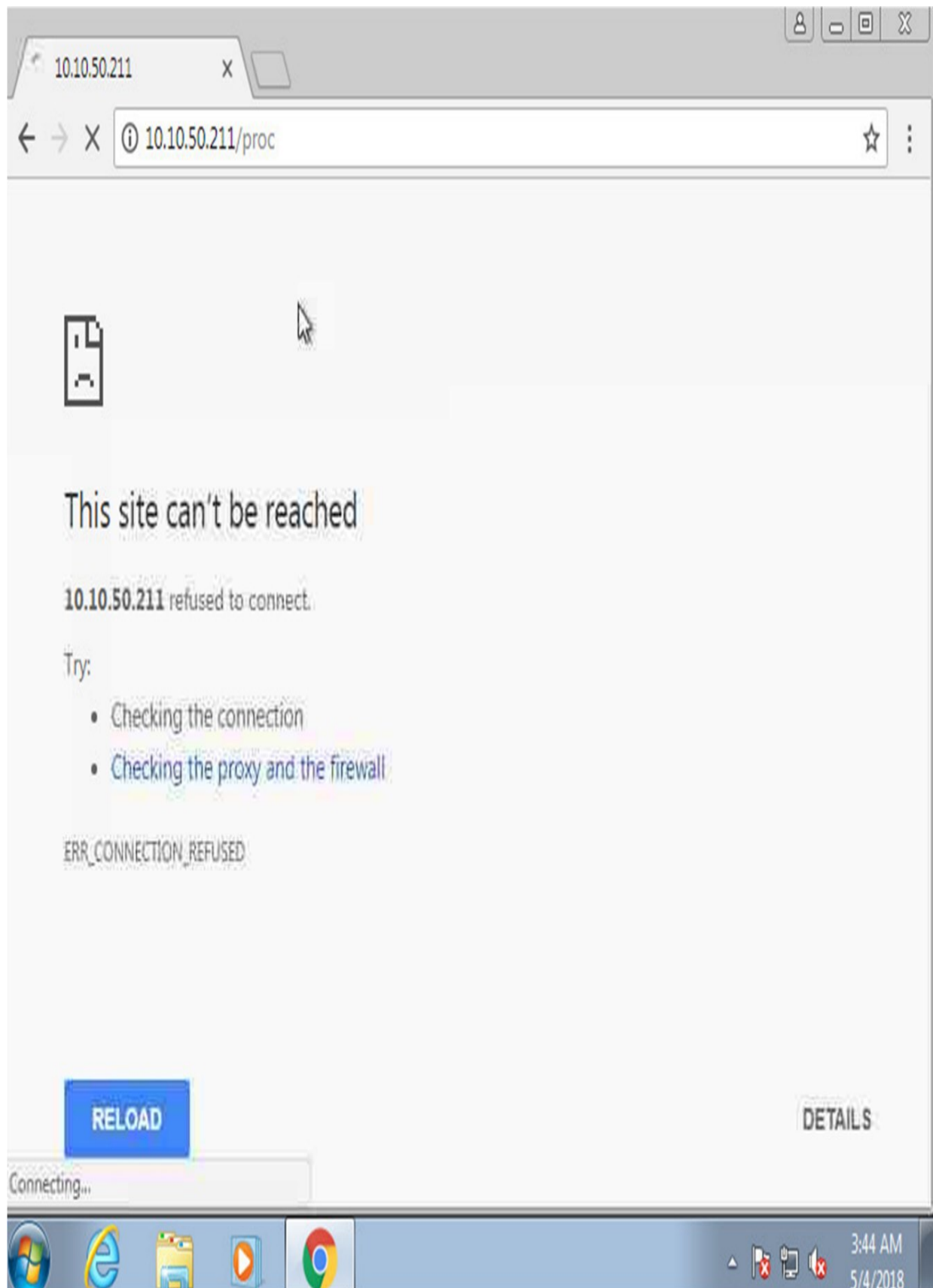
3:44 AM  
5/4/2018





*Figure 7–19: Killing TCP Connection Properties*

6. To verify, retry to establish the connection from Windows 7.



*Figure 7–20: TCP Connection Terminated*  
**Practice Questions**

1. Which of the following statement is the appropriate definition of Malware? A. Malware are Viruses  
B. Malware are Malicious Software  
C. Malware are Trojans  
D. Malware are Infected Files
2. Which of the following does not belongs to the virus? A. Replication  
B. Propagation  
C. Requires trigger to infect  
D. Backdoor
3. Malware Static Analysis is:  
A. Individual analysis of each file  
B. Fragmentation of resources into a binary file for analysis without execution  
C. Fragmentation of resources into a binary file for analysis with the execution  
D. Sandboxing
4. Malware Dynamic Analysis is:  
A. Behavioral Analysis of fragmented file without execution  
B. Behavioral Analysis with the execution of susceptible files  
C. Behavioral Analysis using IDA  
D. Code Analysis by fragmentation
5. Which of the following does not belongs to Trojan deployment? A. Trojan Construction Kit  
B. Dropper  
C. Wrapper  
D. Sniffers
6. \_\_\_\_\_ is used to hide malicious program while creating Trojan. A. Dropper  
B. Wrapper  
C. Crypter  
D. Sniffer