Trojans and Backdoors

Module 6

Engineered by Hackers. Presented by Professionals.
Dangerous Trojan Ransomware Attacks Computers Worldwide

Security researchers have discovered a dangerous piece of ransomware attacking computers around the world.

Experts at the security firm Kaspersky Lab noted that in a blog post today (Nov. 29) that they have been notified of computers infected by ransomware. A type of malware, ransomware holds a computer system – or its data – hostage against its user, and then demands a type of ransom – wiring payment to the hacker or urging the user to buy a fake removal tool, for example -- for its return.


Kaspersky Lab said that, "unlike the previous variants," the new ransomware "doesn't delete files after encryption. Instead it overwrites data in the files, which makes it impossible to use data-recovery software such as PhotoRec, which we suggested during the last attack."

http://www.securitynewsdaily.com
<table>
<thead>
<tr>
<th>Module Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What is a Trojan?</strong></td>
</tr>
<tr>
<td><strong>Overt and Covert Channels</strong></td>
</tr>
<tr>
<td><strong>Purpose of Trojans</strong></td>
</tr>
<tr>
<td><strong>Indications of a Trojan Attack</strong></td>
</tr>
<tr>
<td><strong>Common Ports used by Trojans</strong></td>
</tr>
<tr>
<td><strong>How to Infect Systems Using a Trojan?</strong></td>
</tr>
<tr>
<td><strong>How to Deploy a Trojan?</strong></td>
</tr>
<tr>
<td><strong>Types of Trojans</strong></td>
</tr>
<tr>
<td><strong>How to Detect Trojans?</strong></td>
</tr>
<tr>
<td><strong>Evading Anti-Virus Techniques</strong></td>
</tr>
<tr>
<td><strong>Trojan and Backdoor Countermeasures</strong></td>
</tr>
<tr>
<td><strong>Anti-Trojan Software</strong></td>
</tr>
<tr>
<td><strong>Penetration Testing</strong></td>
</tr>
</tbody>
</table>
What is a Trojan?

- It is a program in which the **malicious or harmful code** is contained inside apparently harmless programming or data in such a way that it can **get control and cause damage**, such as ruining the file allocation table on your hard disk.
- With the help of a Trojan, an attacker gets **access** to the stored passwords in the Trojaned computer and would be able to read **personal documents, delete files** and **display pictures**, and/or **show messages** on the screen.
Overt and Covert Channels

Overt Channel
A legitimate communication path within a computer system, or network, for transfer of data
Example of overt channel includes games or any legitimate programs

Poker.exe
(Valid Application)

Covert Channel
A channel that transfers information within a computer system, or network, in a way that violates the security policy
The simplest form of covert channel is a Trojan

Trojan.exe
(Keylogger Steals Passwords)
Purpose of Trojans

- Steal information such as passwords, security codes, credit card information using keyloggers
- Delete or replace Operating System’s critical files
- Generate fake traffic to create DOS attacks
- Download spyware, adwares and malicious files
- Disable firewalls and antivirus
- Record screenshots, audio and video of victim’s PC
- Infect victim’s PC as a proxy server for relaying attacks
- Use victim’s PC as a botnet to perform DDoS attacks
- Use victim’s PC for spamming and blasting email messages

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
What Do Trojan Creators Look For?

- Credit card information
- Account data (email addresses, passwords, user names, etc.)
- Confidential documents
- Financial data (bank account numbers, social security numbers, insurance information, etc.)
- Calendar information concerning the victim’s whereabouts
- Using the victim’s computer for illegal purposes, such as to hack, scan, flood, or infiltrate other machines on the network or Internet
## Indications of a Trojan Attack

<table>
<thead>
<tr>
<th>Indication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD-ROM drawer opens and closes by itself</td>
<td>The taskbar disappears</td>
</tr>
<tr>
<td>Computer browser is redirected to unknown pages</td>
<td>The account passwords are changed or unauthorized access</td>
</tr>
<tr>
<td>Anti-virus is disabled or does not work properly</td>
<td>Strange purchase statements appear in the credit card bills</td>
</tr>
<tr>
<td>Strange chat boxes appear on victim’s computer</td>
<td></td>
</tr>
<tr>
<td>Windows color settings change</td>
<td>The ISP complains to the victim that his/her computer is IP scanning</td>
</tr>
<tr>
<td>Computer screen flips upside down or inverts</td>
<td></td>
</tr>
<tr>
<td>Screensaver’s settings change automatically</td>
<td>People know too much personal information about a victim</td>
</tr>
<tr>
<td>Wallpaper or background settings change</td>
<td>The computer monitor turns itself off and on</td>
</tr>
<tr>
<td>Functions of the right and left house buttons are reversed</td>
<td>The computer shuts down and powers off by itself</td>
</tr>
<tr>
<td>Documents or messages are printed from the printer themselves</td>
<td>Ctrl+Alt+Del stops working</td>
</tr>
<tr>
<td>Mouse pointer disappears or moves by itself</td>
<td></td>
</tr>
</tbody>
</table>
Common Ports used by Trojans

1 (UDP) - Sockets des Troie
2 - Death
20 - Senna Spy FTP server
22 - Shaft
30 - Agent 40421
110 - ProMall trojan
119 - Happy99
421 - TCP Wrappers trojan
455-456 - Fatal Connections/Hackers Paradise
50 - DRAT
58 - DMSetup
667 - SniperNet
669 - DP trojan
692 - GayOL
1050 - MiniCommand
1080-81 - WinHole
1095, 1097-98 - RAT
1010-12, 1015-16 - Doly Trojan
1255 - Scarab
133 - Farnaz
1807 - SpySender
2115 - Bugs
2155 - Illusion Mailer, Nirvana
2330 - 2338 - Contact
2330 - 2338 - Contact

Module Flow

- Trojan Infection
- Types of Trojans
- Trojan Detection
- Penetration Testing
- Countermeasures
- Anti-Trojan Software
- Trojan Concepts
How to Infect Systems Using a Trojan?

I. Create a new Trojan packet using a Trojan Horse Construction Kit

II. Create a dropper, which is a part in a trojanized packet that installs the malicious code on the target system

Example of a Dropper

**Installation path:** c:\windows\system32\svchosts.exe  
**Autostart:** HKLM\Software\Micro\run\Iexplore.exe

- **Malicious code**
  - Client address: client.attacker.com
  - Dropzone: dropzone.attacker.com

- **Wrapper**
  - File name: my_name.jpg
  - Wrapper data: Graphic file
How to Infect Systems Using a Trojan?

III. Create a wrapper using tools to install Trojan on the victim's computer

IV. Propagate the Trojan

V. Execute the dropper

VI. Execute the damage routine
A wrapper binds a Trojan executable with an innocent looking .EXE application such as games or office applications.

When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapping application in the foreground.

The two programs are wrapped together into a single file.

Attackers might send a birthday greeting that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen.
Wrapper Covert Programs

Kriptomatik

Advance File Joiner
Different Ways a Trojan can Get into a System

- Legitimate "shrink-wrapped" software packaged by a disgruntled employee
- Fake programs
- Downloading files, games, and screen savers from Internet sites
- Untrusted sites and freeware software
- Instant Messenger applications
- IRC (Internet Relay Chat)
- Attachments
- Physical Access
- Browser and email software bugs
- NetBIOS (FileSharing)
How to Deploy a Trojan?

1. Attacker sends an email to victim containing link to Trojan server.
2. Victim clicks the link and immediately connects to Trojan server in Russia.
3. Trojan is sent to the victim.
4. Attacker installs the Trojan infecting their machine.

Computers typically get infected by clicking on a malicious link or opening an e-mail attachment that installs a Trojan on their computers that serves as a back door to criminals who can then command the computer to send spam email.
Evading Anti-Virus Techniques

- Break the Trojan file into multiple pieces and zip them as single file
- Never use Trojans downloaded from the web (anti-virus can detect these easily)
- ALWAYS write your own Trojan and embed it into an application
- Change the content of the Trojan using hex editor and also change the checksum and encrypt the file
- Change Trojan’s syntax:
  - Convert an EXE to VB script
  - Convert an EXE to a DOC file
  - Convert an EXE to a PPT file
  - Convert an EXE to a PDF file
Types of Trojans

- VNC Trojan
- HTTP/HTTPS Trojan
- ICMP Trojan
- Command Shell Trojan
- Data Hiding Trojan
- Destructive Trojan
- Document Trojan
- Covert Channel Trojan
- Botnet Trojan
- Proxy Server Trojan
- Remote Access Trojan
- E-mail Trojan
- FTP Trojan
- GUI Trojan
- SPAM Trojan
- Credit Card Trojan
- Defacement Trojan
- E-banking Trojan
- Notification Trojan
- Mobile Trojan
- MAC OS X Trojan

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Command Shell Trojans

- Command shell Trojan gives remote control of a command shell on a victim’s machine.
- Trojan server is installed on the victim's machine, which opens a port for attacker to connect. The client is installed on the attacker's machine, which is used to launch a command shell on the victim’s machine.

```
C:> nc <ip> <port>
```

```
C:> nc -L -p <port> -t -e cmd.exe
```
Command Shell Trojan: **Netcat**

```
C:\>nc.exe -h
[vl.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
    -d      detach from console, stealth mode
    -e prog inbound program to exec [dangerous!!]
    -g gateway source-routing hop point[s], up to 8
    -G num  source-routing pointer: 4, 8, 12, ...
    -h      this cruft
    -i secs delay interval for lines sent, ports scanned
    -l      listen mode, for inbound connects
    -L      listen harder, re-listen on socket close
    -n      numeric-only IP addresses, no DNS
    -o file hex dump of traffic
    -p port local port number
    -r      randomize local and remote ports
    -s addr local source address
    -t      answer TELNET negotiation
    -u      UDF mode
    -v      verbose [use twice to be more verbose]
    -w secs timeout for connects and final net reads
    -z      zero-I/O mode [used for scanning]

port numbers can be individual or ranges: m-n [inclusive]
```

C:\>
GUI Trojan: MoSucker
GUI Trojan: Jumper and Biodox
VIA LETTER

John Stevens
Royal Communications Company
445 152th Street S.W.
Washington, DC 20554

September 2, 2010

RE: FedEx Shipment Airway Bill Number: 867676340056

Dear Mr. Stevens:

We have received a package addressed to you at the value of USD 2,300. The custom duty has not been paid for this shipment which is listed as Apple iMac 24" Computer.

Please call us at FedEx at 1800-234-446 Ext 345 or e-mail me at m.roberts@fedex.com regarding this shipment.

Please visit our FedEx Package Tracking Website to see more details about this shipment and advice us on how to proceed. The website link is attached with this letter.

Sincerely,
Michelle Roberts
Customer Service Representative
International Shipment and Handling
Fedex Atlanta Division
Tel: 1800-234-446 Ext 345
http://www.fedex.com
m.roberts@fedex.com
**E-mail Trojans**

- Attacker gains remote control of a victim computer by sending email messages.
- Attackers can then retrieve files or folders by sending commands through email.
- Attacker uses open relay SMTP server and fakes the email's FROM field to hide origin.

Diagram:
- **Attacker** sends an email attachment, `calc.exe`, to the victim.
- The attachment is executed, granting the attacker remote control.
- Instructions are sent through emails, bypassing the firewall.
- **Victim** receives the email and opens the attachment, allowing the attacker to gain control.
E-mail Trojans: RemoteByMail
Defacement Trojans

Example of calc.exe: Defaced
- Resource editors allow to view, edit, extract, and replace strings, bitmaps, logos, and icons from any Windows program.

They apply User-styled Custom Applications (UCA) to deface Windows application.

It allows you to view and edit almost any aspect of a compiled Windows program, from the menus to the dialog boxes to the icons and beyond.
Defacement Trojans: **Restorator**
Botnet Trojans

- Botnet Trojans infect a large number of computers across a large geographical area to **create a network of bots** that is controlled through a Command and Control (C&C) center.
- Botnet is used to **launch various attacks** on a victim including denial-of-service attacks, spamming, click fraud, and the theft of financial information.
Botnet Trojan: Illusion Bot
## Botnet Trojan: NetBot Attacker

![NetBot Attacker Interface](image)

### Table: NetBot Attacker Details

<table>
<thead>
<tr>
<th>PC IP</th>
<th>Computer</th>
<th>System</th>
<th>Memory</th>
<th>Service edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>84.123.65.65</td>
<td>CASA</td>
<td>WindowsXP</td>
<td>1025MB</td>
<td>20070313</td>
</tr>
<tr>
<td>84.61.20.243</td>
<td>LE3CH</td>
<td>WindowsXP</td>
<td>769MB</td>
<td>20070313</td>
</tr>
<tr>
<td>88.23.255.207</td>
<td>PC1</td>
<td>WindowsXP</td>
<td>2049MB</td>
<td>20070313</td>
</tr>
<tr>
<td>189.179.71.219</td>
<td>VAIO</td>
<td>WindowsXP</td>
<td>1273MB</td>
<td>20070313</td>
</tr>
<tr>
<td>84.125.150.231</td>
<td>NOMB</td>
<td>WindowsXP</td>
<td>225MB</td>
<td>20070313</td>
</tr>
<tr>
<td>201.222.225.237</td>
<td>khriz</td>
<td>WindowsXP</td>
<td>256MB</td>
<td>20070313</td>
</tr>
<tr>
<td>80.25.176.211</td>
<td>JUAN</td>
<td>WindowsXP</td>
<td>1024MB</td>
<td>20070313</td>
</tr>
<tr>
<td>190.31.125.42</td>
<td>RASTA</td>
<td>WindowsXP</td>
<td>760MB</td>
<td>20070313</td>
</tr>
<tr>
<td>189.149.25.225</td>
<td>MAQUI</td>
<td>WindowsXP</td>
<td>448MB</td>
<td>20070313</td>
</tr>
<tr>
<td>190.198.246.135</td>
<td>BLAK</td>
<td>WindowsXP</td>
<td>225MB</td>
<td>20070313</td>
</tr>
<tr>
<td>81.37.52.182</td>
<td>OSCA</td>
<td>WindowsXP</td>
<td>1025MB</td>
<td>20070313</td>
</tr>
<tr>
<td>84.126.245.140</td>
<td>COLOS</td>
<td>WindowsXP</td>
<td>257MB</td>
<td>20070313</td>
</tr>
</tbody>
</table>

- **Monitor port**: 80
- **Warning team**: [www.hackeroo.com](http://www.hackeroo.com)
- **Had 12 PC on-line**

---

*Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.*
Proxy Server Trojans

- Trojan Proxy is usually a standalone application that allows remote attackers to use the victim’s computer as a proxy to connect to the Internet.
- Proxy server Trojan, when infected, starts a hidden proxy server on the victim’s computer.
- Thousands of machines on the Internet are infected with proxy servers using this technique.
Proxy Server Trojan:
W3bPrOxy Tr0j4nCr34t0r (Funny Name)

W3bPrOxy Tr0j4n is a proxy server Trojan which supports multi-connection from many clients and report IP and ports to mail of the Trojan owner.
FTP Trojans

FTP Trojans install an **FTP server** on the victim's machine, which opens FTP ports.

An attacker can then connect to the **victim's machine** using FTP port to download any files that exist on the victim's computer.
FTP Trojan: **TinyFTPD**

```
C:\Documents and Settings\Admin\Desktop\TinyFTPD 21 55555 test test c:\
win98 all RWLCD
Tiny FTPD V1.4 By WinEggDrop
FTP Server Is Started
ControlPort: 21
BindPort: 55555
UserName: test
Password: test
HomeDir: c:\win98
Allowd IP: all
Local Address: 192.168.168.16
ReadAccess: Yes
WriteAccess: Yes
L1stAccess: Yes
CreateAccess: Yes
DeleteAccess: Yes
ExecuteAccess: Yes
UnlockAccess: No
AnonymousAccess: No
Check Time Out Thread Created Successfully
*************** Waiting For New Connection ***************
0 Connection Is In Use
```
VNC Trojans

- VNC Trojan starts a VNC Server daemon in the infected system
- It connects to the victim using any VNC viewer with the password “secret”
- Since VNC program is considered a utility, this Trojan will never be detected by anti virus

Attacker

Command and control instruction

VNC Traffic

Victim

VNC Server
VNC Trojans

WinVNC

VNC Stealer
HTTP/HTTPS Trojans

**Bypass Firewall**
HTTP Trojans can bypass any firewall and work in the reverse way of a straight HTTP tunnel.

**Spawn a Child Program**
They are executed on the internal host and spawn a child at a predetermined time.

**Access the Internet**
The child program appears to be a user to the firewall so it is allowed to access the Internet.

HTTP request to download a file
Campaign
Trojan passes through HTTP reply
Server
Victim
HTTP Trojan: HTTP RAT

2. Infect the victim’s computer with server.exe and plant HTTP Trojan

3. The Trojan sends an email with the location of an IP address

4. Connect to the IP address using a browser to port 80

- Displays ads, records personal data/keystrokes
- Downloads unsolicited files, disables programs/system
- Floods Internet connection, and distributes threats
- Tracks browsing activities and hijacks Internet browser
- Makes fraudulent claims about spyware detection and removal

Attacker

Victim

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Shttpd Trojan - HTTPS (SSL)

- SHTTPD is a small HTTP Server that can be embedded inside any program.
- It can be wrapped with a genuine program (game `chess.exe`), when executed it will turn a computer into an invisible web server.

Attacker
IP: 10.0.0.5:443

Normally Firewall allows you through port 443

Encrypted Traffic

Victim
IP: 10.0.0.8:443

Connect to the victim using Web Browser
http://10.0.0.5:443

Infect the victim’s computer with `JOUST.EXE`
Shttpd should be running in the background listening on port 443 (SSL)
ICMP Tunneling

Covert channels are methods in which an attacker can hide the data in a protocol that is undetectable.

They rely on techniques called tunneling, which allow one protocol to be carried over another protocol.

ICMP tunneling uses ICMP echo-request and reply to carry a payload and stealthily access or control the victim’s machine.
ICMP Trojan: `icmpsend`

Commands are sent using ICMP protocol

**ICMP Client**
(Command: `icmpsend <victim IP>`)
Remote Access Trojans

This Trojan works like a remote desktop access. Hacker gains complete GUI access to the remote system.

1. Infect (Rebecca’s) computer with `server.exe` and plant Reverse Connecting Trojan
2. The Trojan connects to Port 80 to the attacker in Russia establishing a reverse connection
3. Jason, the attacker, has complete control over Rebecca’s machine
Remote Access Trojan: RAT DarkComet
Remote Access Trojan: Apocalypse
Covert Channel Trojan: CCTT

1. Covert Channel Tunneling Tool (CCTT) Trojan presents various exploitation techniques, creating **arbitrary data transfer channels** in the data streams authorized by a network access control system.

2. It enables attackers to get an **external server shell** from within the internal network and vice-versa.

3. It sets a **TCP/UDP/HTTP CONNECT|POST channel** allowing TCP data streams (SSH, SMTP, POP, etc...) between an external server and a box from within the internal network.
E-banking Trojans

E-banking Trojans intercept a victim's account information before it is encrypted and send it to the attacker's Trojan command and control center.

1. Attacker uploads malicious advertisements.
3. User accesses infected website.
4. The website redirection to the malicious exploit kit.
5. User redirects to malicious exploit kit.
6. The User's PC exploited.
7. Trojan reports for a new bot.
8. Sends instruction to the Trojan.
9. Trojan reports user activities.
10. Instruction to manipulate banks transactions.
11. Reports about successful/failed transaction.
12. User accesses bank A/C.

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Banking Trojan Analysis

1. TAN Grabber
   - Trojan intercepts valid Transaction Authentication Number (TAN) entered by a user
   - It replaces the TAN with a random number that will be rejected by the bank
   - Attacker can misuse the intercepted TAN with the user’s login details

2. HTML Injection
   - Trojan creates fake form fields on e-banking pages
   - Additional fields elicit extra information such as card number and date of birth
   - Attacker can use this information to impersonate and compromise victim’s account

3. Form Grabber
   - Trojan analyses POST requests and responses to victim’s browser
   - It compromises the scramble pad authentication
   - Trojan intercepts scramble pad input as user enters Customer Number and Personal Access Code
E-banking Trojan: ZeuS

ZeuS is a banking Trojan horse program which steal data from infected computers via web browsers and protected storage.
Destructive Trojans

This is a dangerous and destructive type of Trojan

When executed, this Trojan destroys the operating system

This Trojan formats all local and network drives

The user will not be able to boot the Operating System

Format USB Drive, network Drive ....

Format C: \ E: \ F: \ ....

M4sT3r Trojan
Notification Trojans

**Victim’s Location**
Notification Trojan sends the location of the victim’s IP address to the attacker

**Victim’s Activities**
Whenever the victim’s computer connects to the Internet, the attacker receives the notification

**Notification Types**

<table>
<thead>
<tr>
<th>Notification Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIN Notification</td>
<td>Directly notifies the attacker’s server</td>
</tr>
<tr>
<td>ICQ Notification</td>
<td>Notifies the attacker using ICQ channels</td>
</tr>
<tr>
<td>PHP Notification</td>
<td>Sends the data by connecting to PHP server on the attacker’s server</td>
</tr>
<tr>
<td>E-Mail Notification</td>
<td>Sends the notification through email</td>
</tr>
<tr>
<td>Net Send</td>
<td>Notification is sent through net send command</td>
</tr>
<tr>
<td>CGI Notification</td>
<td>Sends the data by connecting to PHP server on the attacker’s server</td>
</tr>
<tr>
<td>IRC Notification</td>
<td>Notifies the attacker using IRC channels</td>
</tr>
</tbody>
</table>
Credit Card Trojans

Credit card Trojans steal victims' credit card related data such as card no., CVV2, and billing details.

Credit card Trojans trick users to visit fake e-banking websites and enter personal information.

Trojan servers transmit the stolen data to remote hackers using email, FTP, IRC, or other methods.

Attacker

Victim

Steals credit card details of victim

Victim

Victim

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Data Hiding Trojans (Encrypted Trojans)

Encryption Trojan encrypts data files in victim's system and renders information unusable

"Your computer caught our software while browsing illegal porn pages, all your documents, text files, databases in the folder My Documents was encrypted with complex password."

Attackers demand a ransom or force victims to make purchases from their online drug stores in return for the password to unlock files

"Do not try to search for a program that encrypted your information – it simply does not exists in your hard disk anymore," pay us the money to unlock the password.
BlackBerry Trojan: PhoneSnoop

PhoneSnoop Trojan remotely activates the microphone of a BlackBerry handheld and listens to sounds near or around it. It can be used to spy on an individual.

1. Install PhoneSnoop (PhoneSnoop.jad)
2. Go to Options ➔ Advanced Options ➔ Applications to select PhoneSnoop application permissions
3. Change the permissions for Input Simulation and Phone to Allow
4. Go to your Downloads or Home Screen and locate the PhoneSnoop icon and start the application
5. Enter the phone number that you want to trigger the remote listening and click Activate

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
MAC OS X Trojan: DNSChanger

This Trojan uses social engineering techniques to make users download the program and run malicious code.

1. User Prompts
   Users are prompted to download a new codec to watch videos.

2. User Downloads
   The user then downloads the codec which actually installs a fake codec.
MAC OS X Trojan: DNSChanger

3. DNS Settings
Local machine's DNS settings are changed to attacker's IP address

4. Playing a Video
After the fake codec is installed, a video is played so as not to raise suspicion

5. HTTP message
A notification is sent to the attacker about the victim's machine using HTTP post message

6. Complete Control
Hackers take complete control of victim's MAC OS X computer
Mac OS X Trojan: Hell Raiser

Note: The complete coverage of MAC OS X hacking is presented in a separate module.

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
How to Detect Trojans?

1. Scan for suspicious OPEN PORTS
2. Scan for suspicious PROCESSES
3. Scan for suspicious RUNNING PROCESSES
4. Scan for suspicious REGISTRY ENTRIES installed on the computer
5. Scan for suspicious DEVICE DRIVERS
6. Scan for suspicious WINDOWS SERVICES
7. Scan for suspicious STARTUP PROGRAMS
8. Scan for suspicious FILES and FOLDERS
9. Scan for suspicious NETWORK ACTIVITIES
10. Scan for suspicious modification to OPERATING SYSTEM FILES
11. Run Trojan SCANNER to detect Trojans

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Scanning for Suspicious Ports

- Trojans open **unused ports** in victim machine to connect back to Trojan handlers.
- Look for the **connection established** to unknown or suspicious IP addresses.

Type `netstat -an` in command prompt.
Port Monitoring Tool: **IceSword**

![Port Monitoring Tool: IceSword](image)

---

**Protocol** | **Local Address** | **Foreign Address** | **State** | **PID** | **PathName**
---|---|---|---|---|---
TCP | 192.168.168.188:8889 | 209.85.153.54:443 | ESTABLISHED | 3076 | D:\Program Files\Mozilla Firefox\firefox.exe
UDP | 192.168.168.188:1000 | *:* | LISTENING | 1076 | D:\Program Files\system32\svchost.exe
TCP | 192.168.168.188:139 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 192.168.168.188:138 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 192.168.168.188:123 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 192.168.168.188:1149 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 127.0.0.1:1000 | *:* | LISTENING | 1076 | D:\Program Files\system32\svchost.exe
UDP | 127.0.0.1:12340 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 127.0.0.1:12346 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 127.0.0.1:12344 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 127.0.0.1:123 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 127.0.0.1:1151 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 127.0.0.1:1106 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 127.0.0.1:1067 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 127.0.0.1:1066 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 127.0.0.1:1065 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 127.0.0.1:1064 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 127.0.0.1:1063 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 127.0.0.1:1062 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 127.0.0.1:7250 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 0.0.0.0:88 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 0.0.0.0:4945 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 0.0.0.0:100 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
UDP | 0.0.0.0:4901 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe
TCP | 0.0.0.0:135 | *:* | LISTENING | 3076 | D:\Program Files\system32\svchost.exe

---

[http://www.antirootkit.com](http://www.antirootkit.com)

---

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Port Monitoring Tools: CurrPorts and TCPView

http://technet.microsoft.com

http://www.nirsoft.net

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Scanning for Suspicious Processes

- Trojans camouflage themselves as genuine Windows services or hide their processes to avoid detection.
- Trojans can also use rootkit methods to hide their processes.
- Trojans inject code into other Windows processes such as explorer.exe to spawn a non-visible iexplorer.exe or firefox.exe process.
- Use process monitoring tools to detect hidden Trojans and backdoors.

Suspicious process: bot.exe
Process Monitoring Tool: What's Running

http://www.whatsrunning.net
Process Monitoring Tools

- PrcView
  http://www.teamcti.com

- HijackThis
  http://free.antivirus.com

- Winsonar
  http://www.fewbyte.com

- HiddenFinder
  http://www.softplatz.com

- Autoruns
  http://technet.microsoft.com

- KillProcess
  http://orangelampsoftware.com

- Security Task Manager
  http://www.neuber.com

- Yet Another (remote) Process Monitor
  http://yaprocmon.sourceforge.net
Scanning for Suspicious Registry Entries

Windows automatically executes instructions in:
- Run
- RunServices
- RunOnce
- RunServicesOnce
- HKEY_CLASSES_ROOT\exe file\shell\open\command "*1" **.

Scanning registry values for suspicious entries may indicate the Trojan infection.

Trojans insert instructions at these sections of registry to perform malicious activities.

NetBus Trojan registry entries
Registry Entry Monitoring Tools

- Registry Fix
  http://www.registrycleanerstested.org

- All-Seeing Eyes
  http://www.fortego.com

- SysAnalyzer
  http://labs.idealend.com

- Regshot
  http://regshot.sourceforge.net

- Registry Shower
  http://www.registryshower.com

- MJ Registry Watcher
  http://www.jacobsrm.com

- Tiny Watcher
  http://kubicle.dcmembers.com

- Active Registry Monitor
  http://www.devicelock.com
Scanning for Suspicious Device Drivers

Trojans are installed along with device drivers downloaded from untrusted sources and use these drivers as a shield to avoid detection.

Scan for suspicious device drivers and verify if they are genuine and downloaded from the publisher's original site.

Go to Run → Type `msinfo32` → System Environment → System Drivers

Attacker
# Device Drivers Monitoring Tools: DriverView

![DriverView Screenshot](http://www.nirsoft.net)

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>File Type</th>
<th>Description</th>
<th>Version</th>
<th>Company</th>
<th>Product Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ndlsapi.sys</td>
<td>0x7f920000</td>
<td>Network Driver</td>
<td>NDIS 3.0 connection wrapper</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>ndisuslo.sys</td>
<td>0x9425000</td>
<td>Network Driver</td>
<td>NDIS User mode I/O Driver</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>ndiswan.sys</td>
<td>0xb92e0000</td>
<td>Network Driver</td>
<td>MS PPP Framing Driver (Strobe)</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>nfd.sys</td>
<td>0x92e6000</td>
<td>System Driver</td>
<td>NDIS Proxy</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>netbios.sys</td>
<td>0xbaf2000</td>
<td>Network Driver</td>
<td>NetBIOS interface driver</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>netbt.sys</td>
<td>0x95f2000</td>
<td>System Driver</td>
<td>MGT Transport driver</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>npf.sys</td>
<td>0x7757000</td>
<td>System Driver</td>
<td>npf.sys (NT5/6 x86) Kernel driver</td>
<td>4.1.0.2001</td>
<td>CACE Technologies</td>
<td>WinPcap</td>
</tr>
<tr>
<td>Npfs.SYS</td>
<td>0x77c7000</td>
<td>System Driver</td>
<td>NPFS Driver</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>ntdll.dll</td>
<td>0x7c00000</td>
<td>Dynamic Link</td>
<td>NT Layer DLL</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>Ntfs.sys</td>
<td>0x7b82000</td>
<td>System Driver</td>
<td>NT File System Driver</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>ntoskrnl.exe</td>
<td>0x8d47000</td>
<td>Application</td>
<td>NT Kernel &amp; System</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>null.sys</td>
<td>0x7a69000</td>
<td>System Driver</td>
<td>NULL Driver</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>parport.sys</td>
<td>0xb3e0000</td>
<td>System Driver</td>
<td>Parallel Port Driver</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>Parmlr.sys</td>
<td>0x770f000</td>
<td>System Driver</td>
<td>Partition Manager</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>parvdm.sys</td>
<td>0x7f9b000</td>
<td>System Driver</td>
<td>VDM Parallel Driver</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>pci.sys</td>
<td>0x7597000</td>
<td>Dynamic Link</td>
<td>NT Plug and Play PCI Enumerator</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>PCIIDSYS.SYS</td>
<td>0x7707000</td>
<td>System Driver</td>
<td>PCI IDE Bus Driver Extension</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>pcnptpcd.sys</td>
<td>0x76f7000</td>
<td>Network Driver</td>
<td>NDIS 5.0 driver</td>
<td>4.38.0 built by</td>
<td>AMD Inc.</td>
<td>AMD PCnet</td>
</tr>
<tr>
<td>portcls.sys</td>
<td>0xb6e4000</td>
<td>Sound Driver</td>
<td>Port Class (Class Driver for Port)</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>psched.sys</td>
<td>0xbad7000</td>
<td>Network Driver</td>
<td>MS QoS Packet Scheduler</td>
<td>5.1.2600.2180</td>
<td>Microsoft Corporation</td>
<td>Windows</td>
</tr>
<tr>
<td>ptt link.sys</td>
<td>0x77f8000</td>
<td>System Driver</td>
<td>Parallel Technologies DirectPort</td>
<td>1.10</td>
<td>Parallel Technologies</td>
<td>DirectPort</td>
</tr>
</tbody>
</table>

[http://www.nirsoft.net](http://www.nirsoft.net)
Device Drivers Monitoring Tools

Driver Detective
http://www.drivershq.com

Driver Magician
http://www.drivermagician.com

Unknown Device Identifier
http://www.zhangduo.com

Driver Reviver
http://www.reviversoft.com

DriverGuide Toolkit
http://www.driverguidetoolkit.com

DriverScanner
http://www.uniblue.com

DriverMax
http://www.innovative-sol.com

Double Driver
http://www.boozet.org

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Scanning for Suspicious Windows Services

Trojans spawn Windows services allow attackers remote control to the victim machine and pass malicious instructions.

Trojans rename their processes to look like a genuine Windows service in order to avoid detection.

Trojans employ rootkit techniques to manipulate HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services registry keys to hide its processes.
Windows Services Monitoring Tools: Windows Service Manager (SrvMan)

http://tools.sysprogs.org
Windows Services Monitoring Tools

- **Smart Utility**
  - [http://mywaywindows.blogspot.com](http://mywaywindows.blogspot.com)

- **ServiWin**
  - [http://www.nirsoft.net](http://www.nirsoft.net)

- **Netwrix Service Monitor**
  - [http://www.netwrix.com](http://www.netwrix.com)

- **Windows Service Manager Tray**
  - [http://www.childhoodcoder.com](http://www.childhoodcoder.com)

- **Service Manager Plus**
  - [http://www.tsachi.net](http://www.tsachi.net)

- **AnVir Task Manager**
  - [http://www.anvir.com](http://www.anvir.com)

- **Vista Services Optimizer**
  - [http://www.smartpcutilities.com](http://www.smartpcutilities.com)

- **Process Hacker**
  - [http://processhacker.sourceforge.net](http://processhacker.sourceforge.net)
Scanning for Suspicious Startup Programs

Check startup folder
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
C:\Users\(User-Name)\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Check startup program entries in the registry
Details are covered in next slide

Check Windows services automatic started
Go to Run → Type services.msc → Sort by Startup Type

Check device drivers automatically loaded
C:\Windows\System32\drivers

Check boot.ini or bcd (bootmgr) entries
Windows 7 Startup Registry Entries

Explorer Startup Setting
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows, load

Windows Startup Setting
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

IE Startup Setting
- HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks
- HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar
- HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions
- HKCU\SOFTWARE\Microsoft\Internet Explorer\MenuExt

Programs that run on Windows startup can be located in these registry entries
Startup Programs Monitoring Tools: Starter

http://codestuff.tripod.com
Startup Programs Monitoring Tools: Security AutoRun

http://tcpmonitor.altervista.org
Startup Programs Monitoring Tools

- Absolute Startup manager
  http://www.absolutestartup.com

- ActiveStartup
  http://www.hexilessoft.com

- StartEd Lite
  http://startedfree.outertech.com

- Startup Tracker
  http://www.dougknox.com

- Startup Inspector
  http://www.windowsstartup.com

- Autoruns
  http://technet.microsoft.com

- Manage PC Startup
  http://www.pc-startup.com

- Program Starter
  http://www.ab-tools.com
Scanning for Suspicious Files and Folders

Trojans normally modify system’s files and folders. Use these tools to detect system changes.

**FCIV**
It is a command line utility that computes MD5 or SHA1 cryptographic hashes for files.

```
C:\CIV>fciv.exe c:\hash.txt
// File Checksum Integrity Verifier version 2.05.
// 6b1fb2f76c139c82253732e1c8824cc2
```

**TRIPWIRE**
It is an enterprise class system integrity verifier that scans and reports critical system files for changes.

**SIGVERIF**
It checks integrity of critical files that have been digitally signed by Microsoft.
Files and Folder Integrity Checker: FastSum and WinMD5

http://www.fastsum.com

http://www.blisstonia.com
Files and Folder Integrity Checker

- MD5 Checksum Verifier
  http://www.flashplayerpro.com

- Advanced CheckSum Verifier (ACSV)
  http://www.irmis.net

- SysInspect
  http://sysinspect.com

- Fsum Fronted
  http://fsumfe.sourceforge.net

- Verisys
  http://www.ionx.co.uk

- AFICK (Another File Integrity Checker)
  http://afick.sourceforge.net

- Sentinel
  http://www.runtimeware.com

- Xintegrity Professional
  http://www.xintegrity.com
Scanning for Suspicious Network Activities

Trojans connect back to handlers and send confidential information to attackers.
Use network scanners and packet sniffers to monitor network traffic going to malicious remote addresses.

Run tools such as Capsa to monitor network traffic and look for suspicious activities sent over the Web.
Detecting Trojans and Worms with **Capsa**

Network Analyzer

Capsa is an intuitive network analyzer, which provides detailed information to help check if there are any **Trojan activities** on a network.
Module Flow

Trojan Infection → Types of Trojans → Trojan Detection → Countermeasures → Anti-Trojan Software

Penetration Testing
# Trojan Countermeasures

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Avoid downloading and executing applications from untrusted sources</td>
</tr>
<tr>
<td>2</td>
<td><strong>Avoid opening email attachments received from unknown senders</strong></td>
</tr>
<tr>
<td>3</td>
<td>Install patches and security updates for the operating systems and applications</td>
</tr>
<tr>
<td>4</td>
<td><strong>Scan CDs and floppy disks with antivirus software before using</strong></td>
</tr>
<tr>
<td>5</td>
<td>Avoid accepting the programs transferred by instant messaging</td>
</tr>
<tr>
<td>6</td>
<td><strong>Block all unnecessary ports at the host and firewall</strong></td>
</tr>
<tr>
<td>7</td>
<td>Harden weak, default configuration settings</td>
</tr>
<tr>
<td>8</td>
<td><strong>Disable unused functionality including protocols and services</strong></td>
</tr>
<tr>
<td>9</td>
<td>Avoid typing the commands blindly and implementing pre-fabricated programs or scripts</td>
</tr>
<tr>
<td>10</td>
<td><strong>Monitor the internal network traffic for odd ports or encrypted traffic</strong></td>
</tr>
<tr>
<td>11</td>
<td>Manage local workstation file integrity through checksums, auditing, and port scanning</td>
</tr>
<tr>
<td>12</td>
<td><strong>Run local versions of anti-virus, firewall, and intrusion detection software on the desktop</strong></td>
</tr>
<tr>
<td>13</td>
<td>Restrict permissions within the desktop environment to prevent malicious applications installation</td>
</tr>
</tbody>
</table>
Backdoor Countermeasures

Detect

Most commercial anti-virus products can automatically scan and detect backdoor programs before they can cause damage

Educate Users

Educate users not to install applications downloaded from untrusted Internet sites and email attachments

Anti-virus Tools

Use anti-virus tools such as Windows Defender, McAfee, and Norton to detect and eliminate backdoors
Trojan Horse Construction Kit

Construct Trojan
Trojan Horse construction kits help attackers to construct Trojan horses of their choice

Trojan Horse Construction Kits

Trojan Horse Construction Kit

Progenic Mail Trojan Construction Kit - PMT

Pandora’s Box

Trojan Execution
The tools in these kits can be dangerous and can backfire if not executed properly
Module Flow

- Trojan Infection
- Types of Trojans
- Trojan Detection
- Countermeasures
- Anti-Trojan Software
- Penetration Testing
Anti-Trojan Software: TrojanHunter

Select Folders to Scan

- Desktop
- Documents
- Computer
- 3.5 Floppy (A:)
- Local Disk (C:)
- CD Drive (D:)
- CD Drive (E:)

Registry scan
No suspicious entries found
Infile scan
No suspicious entries found
Port scan
No suspicious open ports found
Memory scan
No trojans found in memory
File scan (autostarted files, running executables)
No trojan files found

http://www.misec.net
Anti-Trojan Software: **Emsisoft Anti-Malware**

![Emsisoft Anti-Malware Interface](http://www.emsisoft.com)

**Clean Computer**

- Processes scanned: 81
- Files scanned: 2452
- Cookies scanned: 432
- Objects detected: 31

### Scanning:

**Scan finished!**

If there has been Malware found on your PC, you can get more information online about each detected Malware. Click the name of the detected malware to view the description in a new browser window.

Select all objects you want to quarantine and finally click the "Quarantine selected objects" button.

<table>
<thead>
<tr>
<th>Diagnosis</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace.Registry.WhenISearch/A2</td>
<td>1 traces - medium risk</td>
</tr>
<tr>
<td>Trace.Registry.ZeroPopupBar/A2</td>
<td>1 traces - medium risk</td>
</tr>
<tr>
<td>Trace.TrackingCookie.Zo7/A2</td>
<td>1 cookies - low risk</td>
</tr>
<tr>
<td>Trace.TrackingCookie.edtech/A2</td>
<td>2 cookies - low risk</td>
</tr>
<tr>
<td>Trace.TrackingCookie.advertising/A2</td>
<td>1 cookies - low risk</td>
</tr>
</tbody>
</table>

**Suspect files have been detected during the scan.**

- **Quarantine selected objects**
- **Delete selected objects**
- **Save Report**

**Powered by Emsisoft and Ikarus scanning technology**

© 2010 Emsisoft GmbH

All Rights Reserved. Reproduction is Strictly Prohibited.
Anti-Trojan Softwares

- Trojan Guarder
  http://www.your-soft.com

- Anti-Trojan Shield (ATS)
  http://www.atshield.com

- Spyware Doctor
  http://www.pctools.com

- Comodo BOClean
  http://www.comodo.com

- Anti Hacker
  http://www.hide-my-ip.com

- XoftSpySE
  http://www.paretologic.com

- SPYWAREfighter
  http://www.spamfighter.com

- Anti Trojan Elite
  http://www.remove-trojan.com
Pen Testing for Trojans and Backdoors

- **Scan for open ports**
  - Use tools such as IceSword, CurrPorts and TCPView

- **Scan for running Processes**
  - Use tools such as What's Running and HijackThis

- **Scan for registry entries**
  - Use tools such as JV Power Tools and Regshot

- **Scan for device drivers installed on the computer**
  - Use tools such as DriverView and Driver Detective

- **Scan for Windows services**
  - Use tools such as SrvMan and ServiWin

- **Scan the system for open ports**, running processes, registry entries, device drivers and services
- **If any suspicious port, process, registry entry, device driver or service is discovered**, check the associated executable files
- **Collect more information** about these from publisher’s websites, if available, and Internet
- **Check if the open ports are known to be opened by Trojans in wild**
Pen Testing for **Trojans and Backdoors**

1. **Scan for startup programs**
   - Use tools such as Starter, Security AutoRun and Autoruns
   - Check the *startup programs* and determine if all the programs in the list can be recognized with known functionalities

2. **Scan for files and folders**
   - Use tools such as FCIV, TRIPWIRE and SIGVERIF
   - Check the data files for *modification* or *manipulation* by opening several files and comparing hash value of these files with a pre-computed hash

3. **Scan for network activities**
   - Use tools such as Capsa Network Analyzer
   - Check for *suspicious network activities* such as upload of bulk files or unusually high traffic going to a particular web address

4. **Scan for modification to OS files**
   - Use tools such as FCIV and TRIPWIRE
   - Check the *critical OS file* modification or manipulation using tools such as TRIPWIRE or manually comparing hash values if you have a backup copy

5. **Run Trojan Scanner to detect Trojans**
   - Use tools such as Trojan Hunter and Spyware Doctor
   - Run an updated *Trojan scanner* from a reputed vendor to identify Trojans in wild
Pen Testing for Trojans and Backdoors

1. Document all the findings

2. If Trojans are detected?
   - YES
     - Isolate the machine from network
   - NO
     - Update and run antivirus

3. Is updated anti-virus running?
   - YES
     - Find other anti-virus solution to clean Trojans
   - NO
     - Sanitize the complete system for Trojans using an updated anti-virus

- Document all your findings in previous steps; it helps in determining the next action if Trojans are identified in the system.
- Isolate infected system from the network immediately to prevent further infection.
- Sanitize the complete system for Trojans using an updated anti-virus.
Trojans are malicious pieces of code that carry cracker software to a target system.

They are used primarily to gain and retain access on the target system.

They often reside deep in the system and make registry changes that allow it to meet its purpose as a remote administration tool.

Popular Trojans include MoSucker, RemoteByMail, Illusion Bot, HTTP RAT, and Zeus.

Awareness and preventive measures are the best defenses against Trojans.
"Never trust anything that can think for itself if you can't see where it keeps its brain."

- J.K. Rowling,
  An Author