|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 13 |
| Practical 10 |
| **Live Response – Analyzing Volatile Data** | |

**OBJECTIVES**

1. To be able to perform basic live response on a Windows machine.
2. To be able to interpret the results from live response.

Introduction

When a Microsoft Windows machine is involved in an incident, we have several choices of how to proceed in our investigation. The overall scenario usually dictates the next steps an investigator takes. Sometimes your victim cannot afford to remove the system from the network due to certain reasons. Therefore a traditional forensic duplication cannot be acquired. Other times, the data in currently in memory may be the only evidence of the incident.

Live response collects all of the relevant data from the system that will be used to confirm whether an incident occurred. The data collected during a live response consists of *Volatile* and *Nonvolatile* data.

The volatile data of a victim computer usually contains significant information that helps us determine the “who”, “how”, and possibly “why” of the incident. To help answer these questions, we will be collecting data from the following areas:

* The System Date and Time
* Current Network Connections
* Open TCP or UDP Ports
* Which Executables are opening TCP or UDP ports
* Users Currently Logged On
* Running Processes
* Modification, Creation, and Access times of Files

Activities

1. System Date and Time

Boot up the lab machine (or your own laptop) to Windows 10. Start the DOS command line and enter the following commands:

* date /t
* time /t

A-1: Record the results below.

Date /t showed the current date

Time/t showed the current time

1. Current Network Collections

It is entirely possible that we could be executing live response process while the attacker is connected to the server. It could also be possible that the attacker is running a brute force mechanism against other machines on the Internet from this server.

To view the machine’s network connections, issue the netstat command as follows:

* netstat –an

Q1: What does the option “-an” mean?

Shows all other connections that are not “ESTABLISHED”

The information that is displayed includes the Protocol, the Local Address, the Foreign (remote) Address, and the connection State. The IP addresses also display the port number, after a colon (:). The possible values for State are shown in the table below.

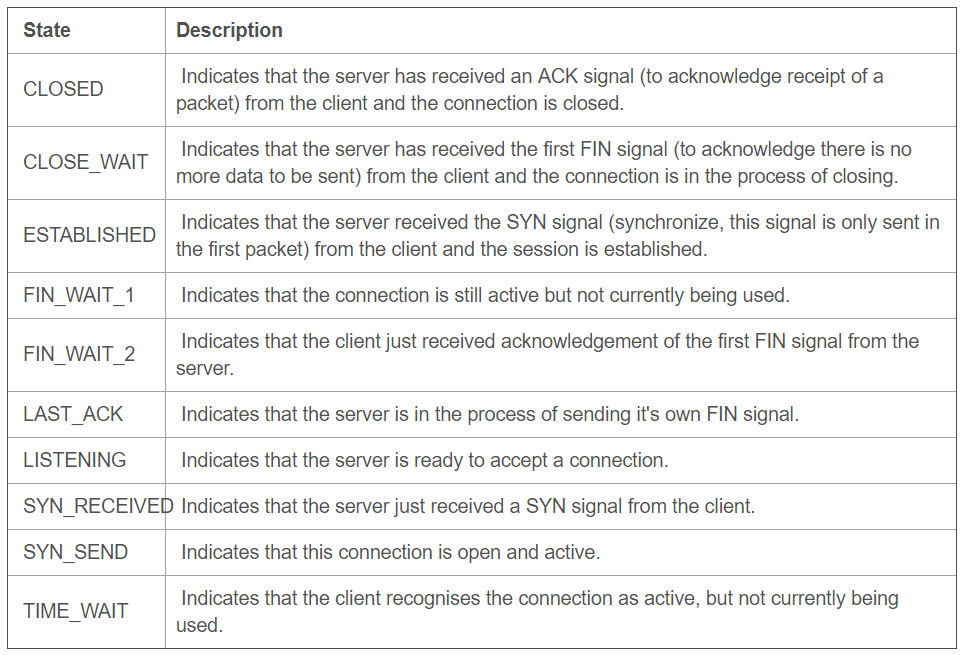


Table 1: Connection State

Guidelines to interpret the results:

* In lines saying 'ESTABLISHED', you need the **remote port** to identify what has connected to the remote site.
* In lines saying 'LISTENING', you need the **local port** to identify what is listening there.
* Each outbound TCP connection also causes a LISTENING entry on the same port.
* Most UDP listening ports are duplicates from a listening TCP port. Ignore them unless they don't have a TCP twin.
* TIME\_WAIT entries are not important.
* If it says **0.0.0.0** on the Local Address column, it means that port is listening on all 'network interfaces' (i.e. your computer, your modem(s) and your network card(s)).
* If it says **127.0.0.1** on the Local Address column, it means that port is ONLY listening for connections from your PC itself, not from the Internet or network. No danger there.
* If it displays **your online IP** on the Local Address column, it means that port is ONLY listening for connections from the Internet.

Now, redirect the netstat results in a text file:

* netstat –an > netstat\_output.txt

B-1: Open the netstat\_output.txt and select those entries that you feel that are suspicious and worth more attention.

1. Open TCP or UDP Ports

An open rogue port usually denotes a backdoor running on the victim machine. Windows opens a lot of legitimate ports during the course of doing its business.

Refer to the following website for the list of well-known ports:

<https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers>

Port 1 to 515 are normal Windows ports, typically started when TCP/IP services are installed on the machine. The rest of the Listening TCP ports are ephemeral ports.

Q2: What is an ephemeral port?

C-1: Select those entries that you feel that are suspicious and worth more attention.

Some of the above ports could be legitimate, but some could also be ports onto which attacker has attached a backdoor. With netstat alone, we cannot identify the purpose of the open ports. We need to see which executables opened the ports to get a better idea of their purposes.

1. Executables Opening TCP or UDP Ports

To examine the strange ports that are open on the machine, we must link the open ports to the executables that opened them.

Let’s make use of CurrPorts tool to examine the open ports.

Download cports.zip from Brightspace, unzip it and execute cports.exe. The tool will give very detailed information about the executables that opened the ports.

Rearrange and sort the columns in such a way that Process Name, PID, Protocol etc. are next to each other. Sort the Local Address column.

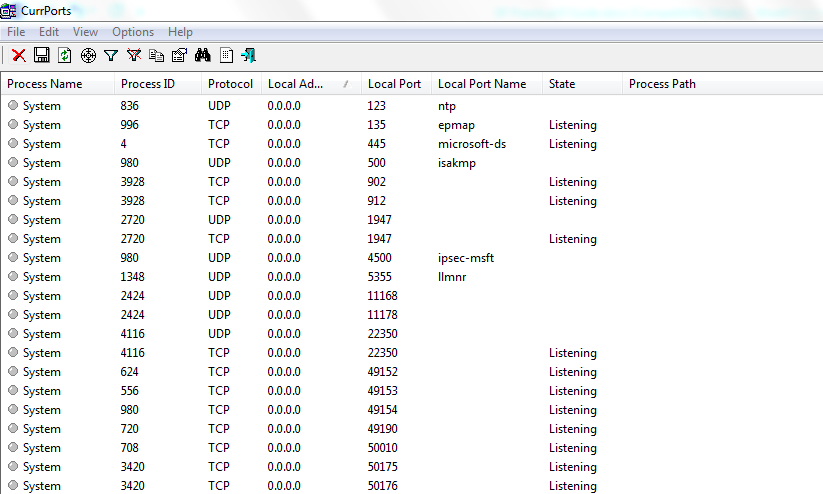


Figure 1: CurrPorts

D-1: From the list of Listening ports, are there any suspicious rogue ports? (You may need to Google to find out the suspicious process/executables)

1. Users Currently Logged On

To stay stealthy during live response, we could run PSLoggedOn. The tools will return the users that are currently logged onto the system or accessing the resource shares.

Download PSTools.zip from Brightspace and extract it to a folder. From command prompt, navigate to the folder where it is located and enter

* Psloggedon

E-1: Who are users currently logged on the victim’s machine?

1. Running Processes

Ultimately, we want to know what processes attacker executed on victim’s machine because they could contain backdoors. Generally, it you are investigating a server that has been started and running for a long time, the legitimate system processes would have long Elapsed Time, an indication of processes running since startup.

The processes that have short Elapsed Time could be started by attacker.

From command prompt, navigate to the folder where PSTools suite is located and enter

* pslist

F-1: Are there any suspicious processes?

1. Modification, Creation, and Access times of Files

Use the *dir* command to get a directory listing of all the files on the target system, recording their size, access(a), modification(w), and creation(c) times.

From command prompt, enter

* dir /t:a
* dir /t:w
* dir /t:c

G-1: Observe the difference in the results among the 3 commands and state your observation below.

Reflection: What have you learnt through this practical exercise?

Reference

* Keith J. Jones, Richard Bejtlich, Curtis W. Rose, *Real Digital Forensics, Computer Security & Incident Response*, Addison-Wesley*.*

- The End -