

## **Lab 10 Report**

Jason Tolbert

The Pennsylvania State University

IST 894-001: Capstone Experience

Dr. Michael Bartolacci, Instructor

April 6<sup>th</sup>, 2025

## Table of Contents

<b>General Overview.....</b>	<b>3</b>
Digital Forensics.....	3
Indicators of Compromise.....	4
<b>Technical Overview .....</b>	<b>5</b>
Digital Forensics.....	5
Indicators of Compromise.....	5
<b>References .....</b>	<b>7</b>
<b>Screenshots .....</b>	<b>8</b>

# General Overview

This lab introduces participants to essential skills in both digital forensics and the identification of indicators of compromise.

## Digital Forensics

The first part of the lab teaches participants basic digital forensics skills. Digital forensics is the practice of collecting and investigating media stored on computers or sent over networks, typically with the intent of using it as evidence of a crime. Key to investigating any crime is the preservation of evidence. The lab introduces participants to one of the primary ways digital evidence is preserved — hashing.

Hashing is a process that takes the contents of a file and outputs a string of characters called a hash. A given hash can only be produced by the file it was created from; if that file changes, even a little bit, the hash it produces will also change. Thus, if you have the hash of a file, and want to determine whether that file has been altered in the time since you hashed it, you can rehash the file in its current state and compare the new hash to the one you originally took; if they differ, the file has been altered. This makes hashing a highly effective tool for determining whether digital evidence has been tampered with (Premanand Narasimhan & Dr.N.Kala, 2024).

Once participants are familiarized with preserving evidence, the focus of the lab turns to capturing it. Participants are shown how to use command-line tools to capture traffic being sent over a network for later review. In the real world, these kinds of tools provide investigators with a perpetual snapshot of all activity on a network within a given window of time, and are commonly-used to reconstruct the events of computer crimes (Sikos, 2020).

## Indicators of Compromise

The second part of the lab focuses on detecting indicators of compromise – signs that a security breach may have happened or be happening. Participants are taught how to spot these signs, respond to them, and clean up any damage.

Threat hunting, broadly, is about identifying and investigating behavior that looks like it shouldn't be happening (Mahboubi et al., 2024). To that end, participants begin their search for indicators of compromise by looking for new or unauthorized behavior on their system. Participants eventually uncover the presence of a malicious script that forcibly opens their machine to network traffic and a scheduled task that runs said script at regular intervals. Once they discover the backdoor, they move to shut it down, deleting the script and the task that executes it. This approach is a point-for-point mirror of the standard real-world cyber incident response playbook – identify the threat, contain it, eradicate it, and then return the system to a safe state (Cybersecurity and Infrastructure Security Agency, n.d.).



# Technical Overview

This lab introduces participants to essential skills and digital forensics and the identification of indicators of compromise.

## Digital Forensics

The first part of the lab gives participants a practical introduction the forensic analysis of digital information. Participants use tcpdump capture live network traffic, learning how to tailor the interface and duration of the capture session and save the captured data to a pcap file. They then review the pcap file in Wireshark, using its filtering capabilities to isolate unencrypted Telnet traffic and inspect it to find plaintext credentials that were used to execute a successful login to a remote machine.

Once participants acquire their first piece of digital evidence – the pcap file – they learn how to preserve it using hashing. Using both md5sum and shasum, participants how to apply hashes to verify that the packet capture has not been altered between acquisition and examination.

## Indicators of Compromise

The second part of the lab focuses on identifying indicators of compromise on a system that has already been breached. Participants meticulously scour the system for evidence

of unusual behavior. They begin with relatively obvious checks, like examining authentication logs for suspicious login activity, and looking through shell history for possibly malicious commands. They continue to search for compromise in places that are not as easily visible, using `ps`, `netstat`, and `iftop` to analyze active processes and network connections. Through `iftop`, they discover that the attacker has gained persistent access to their machine via SSH.

During their investigation, participants find a malicious script that forcibly opens port 7777 and a cron job that runs said script every minute. After deleting the script and removing the cron job, they move to fully return their machine to a secure state by deleting the attacker's SSH key.

## References

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cybersecurity incident & vulnerability response playbooks*.

Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., & Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, 232, 104004. <https://doi.org/10.1016/j.jnca.2024.104004>

Premanand Narasimhan & Dr.N.Kala. (2024). Ensuring the integrity of digital evidence: The role of the chain of custody in digital forensics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(6), 2438–2450. <https://doi.org/10.32628/CSEIT2410612443>

Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, 32, 200892. <https://doi.org/10.1016/j.fsidi.2019.200892>

# Screenshots

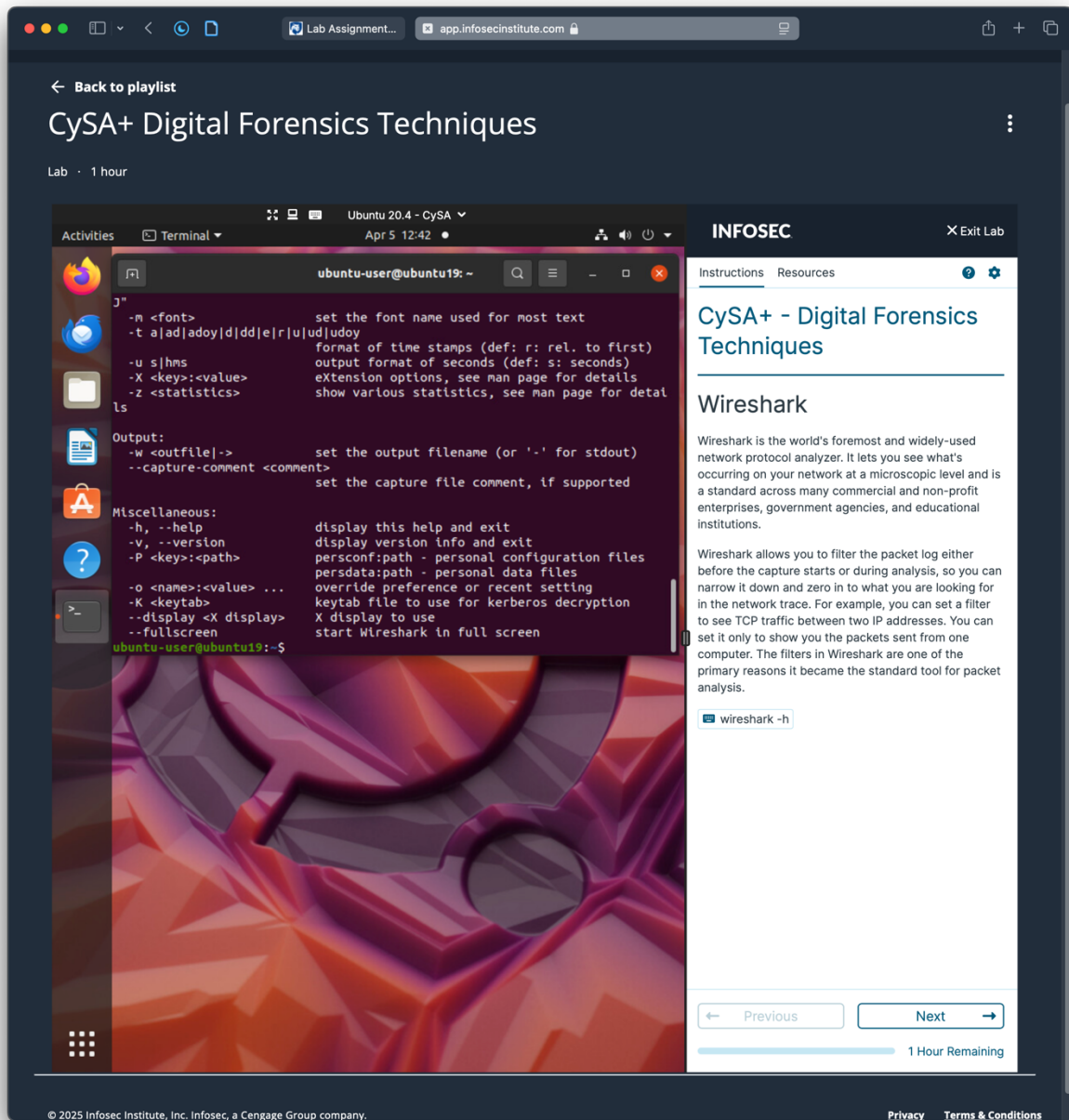


Figure 1. The Wireshark help text.

Back to playlist

CySA+ Digital Forensics Techniques

Lab · 1 hour

ActivitiesTerminalUbuntu 20.4 - CySAApr 5 12:44

ubuntu-user@ubuntu19: ~

ubuntu-user@ubuntu19:~\$ touch file1

ubuntu-user@ubuntu19:~\$ sha256sum file1

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 file1

ubuntu-user@ubuntu19:~\$

INFOSEC

InstructionsResources

SHA-3, and BLAKE2 became vital tools in cryptography. They are used to construct digital signatures, verify integrity, protect passwords, enable public-key encryption, and more. Cryptographic hash functions differ from non-cryptographic, hash functions used in data structures because they provide security features, which are not available in non-cryptographic hash functions.

Today, hash functions are widely used in various systems. For example, decentralized technologies like Bitcoin and Ethereum rely on cryptographic hash functions to secure the system and maintain the integrity of transactions. Similarly, Git version control uses hash functions combined with Merkle Trees to track code changes.

Another significant application of hashing algorithms is digital signatures. Digital signatures use mathematical cryptographic methods to provide authenticity and integrity to information. They are so reliable and secure that they are considered legally binding in many countries, just like traditional handwritten signatures. Digital signatures are created using public-key cryptography.

touch file1

sha256sum file1

Which of the following is a primary purpose of hashing files?

☐ To compress file size for faster transmission

☐ To encrypt file contents for enhanced security

☐ To verify data integrity and detect alterations

☐ To convert files into a human-readable format

Check

PreviousNext

57 Minutes Remaining

© 2025 Infosec Institute, Inc. Infosec, a Cengage Group company.

PrivacyTerms & Conditions

Figure 2. Creating file1 and reading its SHA-256 hash.

Back to playlist

# CySA+ Digital Forensics Techniques

Lab · 1 hour

Activities

Terminal

Ubuntu 20.4 - CySA

Apr 5 12:46

ubuntu-user@ubuntu19: ~

```
:668, ack 56, win 510, options [nop,nop,TS val 2139019633 ecr 2191071607],
length 409
12:46:13.221295 IP 172.20.1.11.46420 > student.telnet: Flags [.], ack 668,
win 501, options [nop,nop,TS val 2191071607 ecr 2139019633], length 0
12:46:13.221304 IP student.telnet > 172.20.1.11.46420: Flags [P.], seq 668
:734, ack 56, win 510, options [nop,nop,TS val 2139019633 ecr 2191071607],
length 66
12:46:13.221353 IP 172.20.1.11.46420 > student.telnet: Flags [.], ack 734,
win 501, options [nop,nop,TS val 2191071607 ecr 2139019633], length 0
12:46:13.221509 IP student.telnet > 172.20.1.11.46420: Flags [P.], seq 734
:736, ack 56, win 510, options [nop,nop,TS val 2139019633 ecr 2191071607],
length 2
12:46:13.221571 IP 172.20.1.11.46420 > student.telnet: Flags [.], ack 736,
win 501, options [nop,nop,TS val 2191071607 ecr 2139019633], length 0
12:46:13.283186 IP student.telnet > 172.20.1.11.46420: Flags [P.], seq 736
:760, ack 56, win 510, options [nop,nop,TS val 2139019695 ecr 2191071607],
length 24
12:46:13.283393 IP 172.20.1.11.46420 > student.telnet: Flags [.], ack 760,
win 501, options [nop,nop,TS val 2191071669 ecr 2139019695], length 0
12:46:15.160099 ARP, Request who-has lodSense.localdomain tell student, le
ngth 28
12:46:15.160340 ARP, Reply lodSense.localdomain is-at 00:0c:29:14:bc:fc (o
ut Unknown), length 46
```

INFOSEC

Exit Lab

Instructions Resources

## Interception

One of the simplest filters that can be applied to `tcpdump` is `-i`, which is used to specify the network interface name. To list all interfaces, use the `-D` option.

```
tcpdump -D
```

The "any" option will capture traffic in all available interfaces.

To start capturing data, execute the following command:

```
sudo tcpdump -i ens32
```

It will be tough to follow all the requests and identify critical components because everything will be printed on the terminal. To write the information in a file, use the `-w` option followed by a filename. To follow the examples throughout this lab, use the same file names as shown in the command examples.

To stop capturing traffic, press CTRL and C at the same time.

How many interfaces are currently running?

☐ 2

☐ 3

☐ 4

☐ 7

Check

Previous Next

56 Minutes Remaining

© 2025 Infosec Institute, Inc. Infosec, a Cengage Group company.

Privacy Terms & Conditions

Figure 3. Capturing traffic with tcpdump.

The screenshot displays the INFOSEC Skills web application interface. At the top, the navigation bar includes the 'INFOSEC Skills' logo, links for 'Learn', 'Roles', 'Teams', and 'Navigator', and a 'Beta' badge. The main content area is titled 'CySA+ Digital Forensics Techniques' and indicates a 'Lab · 1 hour' duration. A 'Back to playlist' link is visible in the top left of the lab area.

The central focus is a terminal window titled 'Ubuntu 20.4 - CySA'. The terminal shows the following commands and output:

```
ubuntu-user@ubuntu19: ~  
ubuntu-user@ubuntu19:~$ sudo timeout 20 tcpdump -i ens32 -w /home/ubuntu-user/data.pcap  
[sudo] password for ubuntu-user:  
tcpdump: listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
```

To the right of the terminal, the 'INFOSEC' sidebar provides instructions and resources. It explains that 'Tcpdump can be executed with a time limit if used with a UNIX command called timeout. The duration can be a positive integer or a floating-point number, followed by an optional unit suffix:'

- s - seconds (default)
- m - minutes
- h - hours
- d - days

It then instructs the user to 'Open a new terminal window and execute the following command:' and provides a code block:

```
sudo timeout 20 tcpdump -i ens32 -w /home/ubuntu-user/data.pcap
```

Below this, a question is posed: 'What does the -i ens32 option specify in the tcpdump command'. Four radio button options are provided:

- ☐ The output file where the captured data is saved
- ☐ The format of the captured data
- ☐ The duration of the packet capture
- ☐ The network interface to listen to for capturing packets

A green 'Check' button is located below the options. At the bottom of the sidebar, there are 'Previous' and 'Next' navigation buttons, and a progress indicator showing '39 Minutes Remaining'.

Figure 4. Running tcpdump with a 20-second time limit.



The screenshot displays the INFOSEC Skills web application interface. At the top, the navigation bar includes the 'INFOSEC Skills' logo, links for 'Learn', 'Roles', 'Teams', and 'Navigator', and a 'Beta' badge. The main content area is titled 'CySA+ Digital Forensics Techniques' and indicates a 'Lab · 1 hour' duration. A 'Back to playlist' link is located at the top left of the lab content.

The central part of the interface features a terminal window titled 'Ubuntu 20.4 - CySA'. The terminal shows the following commands and output:

```
ubuntu-user@ubuntu19: ~  
ubuntu-user@ubuntu19:~$ sudo timeout 20 tcpdump -i ens32 -w /home/ubuntu-user/data.pcap  
[sudo] password for ubuntu-user:  
tcpdump: listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
```

To the right of the terminal is a quiz section titled 'INFOSEC'. It includes tabs for 'Instructions' and 'Resources'. The 'Instructions' tab contains the following text:

Tcpdump can be executed with a time limit if used with a UNIX command called timeout. The duration can be a positive integer or a floating-point number, followed by an optional unit suffix:

- s - seconds (default)
- m - minutes
- h - hours
- d - days

Open a new terminal window and execute the following command:

```
sudo timeout 20 tcpdump -i ens32 -w /home/ubuntu-user/data.pcap
```

What does the -i ens32 option specify in the tcpdump command

- ☐ The output file where the captured data is saved
- ☐ The format of the captured data
- ☐ The duration of the packet capture
- ☐ The network interface to listen to for capturing packets

A green 'Check' button is located below the options. At the bottom of the quiz section, there are 'Previous' and 'Next' buttons, and a progress indicator showing '39 Minutes Remaining'.

Figure 5. Observing the contents of the data.pcap file in Wireshark.



Lab Assignment...app.infosecinstitute.com

← Back to playlist

CySA+ Indicators of Compromise

Lab · 1 hour

Ubuntu 20.4 -CySA target

ActivitiesTerminalApr 5 13:28

root@ubuntu19:~  
root@ubuntu19:~# cat /backdoor.sh  
#!/bin/bash  
ncat -lp 7777 -e /bin/bash  
root@ubuntu19:~#

INFOSEC

Exit Lab

InstructionsResources

Backdoor

The result shows a shell script named *backdoor.sh*.

Use the cat command to display the content of the script:

cat /backdoor.sh

It looks like the attacker is using the *backdoor.sh* script to open a port on the machine and execute */bin/bash*. This allows the attacker to execute bash commands remotely. We can quickly identify if port 7777 is open using netstat. In computing, netstat is a command-line network utility that displays network connections for Transmission Control Protocol, routing tables, and a number of network interface and network protocol statistics.

The following netstat options can be used to list all listening ports:

- l (listening) - displays listening server sockets
- n (numeric) - does not resolve names
- t (TCP) - show TCP ports
- p (programs) - display PID/Program name for sockets

netstat -lntp

Considering that the -p argument provides the application process id, we can quickly terminate the process, but always be cautious of your actions. What if there is another process that is automatically executing the *backdoor.sh* script, and providing the attacker a persistence to the infrastructure?

On which port is the ncat listener running?

← PreviousNext →

1 Hour Remaining

© 2025 Infosec Institute, Inc. Infosec, a Cengage Group company.

PrivacyTerms & Conditions

Figure 6. Reading the contents of backdoor.sh.



Lab Assignment...app.infosecinstitute.com

INFOSEC SKILLS

LEARNNOTESREADTIPSNAVIGATOR

Back to playlist

CySA+ Indicators of Compromise

Lab · 1 hour

Ubuntu 20.4 -CySA target

ActivitiesTerminalApr 5 13:30

root@ubuntu19: ~

12.5Kb25.0Kb37.5Kb50.0Kb62.5Kb

TX:	cur:	0B	peak:	0B	rates:	0B	0B	0B
RX:	0B	0B	0B	0B	0B	0B	0B	0B
TOTAL:	0B	0B	0B	0B	0B	0B	0B	0B

INFOSEC

Exit Lab

InstructionsResources

From the previous network status shown using the `netstat` command, we know that there is no established connection on port 7777, meaning that the port is accessible, but there are no active connections. Since the backdoor is not being used, it is safe to assume that the attacker is exploiting the systems through other compromised components.

The Secure Shell Protocol (SSH) is often used for administration purposes. The `w` command shows logged users and will list any remote connections on the SSH protocol if there are any.

Since it cannot be predicted when an attacker will decide to connect to the target, the system should be monitored continuously.

w

iftop

We can verify that by analyzing the network traffic using *iftop*, a free software command-line system monitoring tool that produces a frequently updated list of network connections.

`iftop -n -i ens32`

It looks like a host is persistently connecting to our system. Because the `scp` command uses the SSH protocol for authentication, the attacker may have compromised the SSH protocol and added his public key for login to the system.

Which host is persistently connecting to our system?

Check

Previous

Next

58 Minutes Remaining

Figure 8. Monitoring network traffic with iftop.

INFOSEC Skills

Learn Roles Teams Navigator Beta

Back to playlist

CySA+ Indicators of Compromise

Lab · 1 hour

Ubuntu 20.4 -CySA target

Activities

Terminal

Apr 5 13:31

ubuntu-user

root@ubuntu19: ~

GNU nano 4.8 /etc/ssh/sshd\_config

\$OpenSSH: sshd\_config.v.1.103 2018/04/09 20:41:22 tJ Exp 5

# This is the sshd server system-wide configuration file. See

# sshd\_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd\_config shipped with

# OpenSSH is to specify options with their default value where

# possible, but leave them commented. Uncommented options override the

# default value.

Include /etc/ssh/sshd\_config.d/\*.conf

#Port 22

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

#HostKey /etc/ssh/ssh\_host\_rsa\_key

Read 123 lines

Get Help Write Out Where Is Cut Text Justify Cur Pos

Exit Read File Replace Paste Text To Spell Go To Line

INFOSEC

Exit Lab

Instructions Resources

SSH Keys

An SSH key is an access credential in the SSH protocol. Its function is similar to that of usernames and passwords, but the keys are primarily used for automated processes and for implementing single sign-on by system administrators and power users.

Is /home/ubuntu-user/.ssh/

You can use the `ls` command followed by the full path to check for the `authorized_keys` file, but it appears it is missing.

The SSH directory is typically the default location checked when managing keys. However, attackers often avoid common directories to evade detection. Additionally, like many applications, SSH has a configuration file that allows advanced users to customize its behavior and enable additional features.

nano /etc/ssh/sshd\_config

The `authorized_keys` line in the `sshd_config` file specifies the path containing the keys of all authorized users. These users can then authenticate remotely to SSH, gaining access to the target machine.

In which directory is the `authorized_keys` configuration saved?

Check

Previous Next

57 Minutes Remaining

Figure 9. Examining the SSH server configuration file.

Back to playlist

# CySA+ Indicators of Compromise

Lab · 1 hour

ActivitiesTerminalUbuntu 20.4 -CySA targetApr 5 14:13

ubuntu-user

root@ubuntu19: ~

GNU nano 4.8 /tmp/crontab.aUgmyM/crontabModified

Get HelpWrite OutWhere IsCut TextJustifyExitRead FileReplacePaste TextTo Spell

INFOSECExit Lab

InstructionsResources

## Response

Even a minor security breach can have a significant impact. Taking immediate action will help you contain or reduce the effects of a cyber attack.

**Important Note:** Many countries require businesses to notify customers if their information may have been compromised. Be sure to familiarize yourself with applicable laws regarding notification obligations and include this in your response plan.

Even if a cyber incident appears under control, stay vigilant. Attackers often return to previously compromised networks, and despite your efforts, they may find another way in.

...less

After detecting the incident, it's crucial to respond. We've identified a cron job running under the root user that executes `backdoor.sh` and opens port 7777.

Use the `crontab -e` command to remove the line `* * * * * root sh /backdoor.sh 2>&1` and save your changes before exiting.

You can use both nano and gedit to edit the file's content.

Which command is used to edit the crontab?

Check

PreviousNext

27 Minutes Remaining

© 2025 Infosec Institute, Inc. Infosec, a Cengage Group company.

[Privacy](#) [Terms & Conditions](#)

Figure 10. The crontab file, newly empty now that the malicious cron job depicted in Figure 7 has been removed.