

CHAPTER 19

**INCIDENT RESPONSE**

CERTIFIED CYBERSECURITY TECHNICIAN

# INDEX

## Chapter 19: **Incident Response**

<b>Exercise 1:</b> Conduct Security Checks using buck-security on Linux	<b>05</b>
-----	
<b>Exercise 2:</b> Analysis and Validation of Malware Incident	<b>12</b>
-----	
<b>Exercise 3:</b> Implement Policies using Group Policy Management Console	<b>26</b>

## SCENARIO

Information security incidents have sharply increased in recent years, owing to the adoption of digital technologies and the frequent innovation of new technologies. In this environment, organizations are at risk of huge losses in data, trust, profits, systems, devices, and human resources. Therefore, it is crucial for organizations to be prepared to battle—if not completely prevent—these incidents. Understanding the concept of incident response (IR) will help in handling security breaches effectively and minimize the damage due to a cybersecurity attack.

Hence, a security professional, must understand the complete process of incident handling and response (IH&R) that must be implemented to face, fight, and prevent different types of information-based attacks.

## OBJECTIVE

The objective of this lab is to provide expert knowledge on the incident response process. It includes of the following tasks:

- Conducting security checks on Linux using buck-security tool
- Analyzing and validation of malware incident
- Implementing policies using Group Policy Management Conso

## OVERVIEW OF INCIDENT RESPONSE

Incident response (IR) is the process of taking organized and careful steps when reacting to a security incident. It involves a sequence of steps that begin with first identifying and reporting an incident. IR is a systematic approach that is adopted to handle security incidents with minimal damage, recovery time, and costs. In the process of responding to an incident, security professionals can acquire information such as the network vulnerability that allowed the attack, the individual(s) who initiated the attack, and the types of devices and files that were affected. IR processes differ from organization to organization according to their business and operating environment.

## LAB TASKS

A cyber security professional or a security professional use numerous tools and techniques to perform incident response. The recommended labs that will assist in learning the IR process include the following:

**01**

**Conduct Security Checks using buck-security on Linux**

**02**

**Analysis and Validation of Malware Incident**

**03**

**Implement Policies using Group Policy Management Console**

**Note:** Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

## EXERCISE 1: CONDUCT SECURITY CHECKS USING BUCK-SECURITY ON LINUX

Windows OS tracks various events, activities, and functions through logs.

### LAB SCENARIO

Once a security incident has been reported, the IH&R team must perform incident triage. As part of incident triage, security professionals assess the details and correlate indicators with logs and other system files to validate the incident and determine the impacted systems, networks, devices, and applications.

For classifying an incident's severity, security professionals must perform incident analysis and validation to analyze the indicators of a reported issue and verify whether it is an information security incident or an error in hardware or software components. If the reported incident is an information security incident, then the security professionals must perform further analysis to identify any security loopholes that led to the incident.

A security professional must be able to perform security scanning using automated tools to detect security vulnerabilities in operating systems such as Linux and Windows that led to the security incident.

### OBJECTIVE

This lab demonstrates how to conduct security checks using buck-security on Linux operating system to know the security status of the system.

### OVERVIEW OF BUCK-SECURITY

The buck-security tool is a collection of security checks for Linux. It was designed for Debian and Ubuntu servers, but it can be useful for any Linux system. The buck-security tool allows security professionals to identify the security status of a system. It provides an overview of the system's security status within a couple of minutes.

Note: Ensure that the PfSense Firewall virtual machine is running.

1. Turn on the Attacker Machine-2 virtual machine.

2. In the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.

Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.

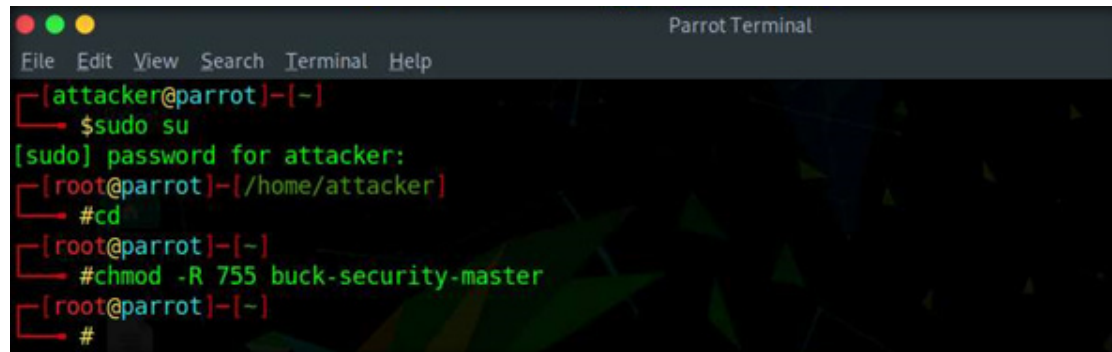
Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.

3. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.

4. A Parrot Terminal window appears. In the terminal window, type `sudo su` and press Enter to run the programs as a root user.

# EXERCISE 1: CONDUCT SECURITY CHECKS USING BUCK-SECURITY ON LINUX

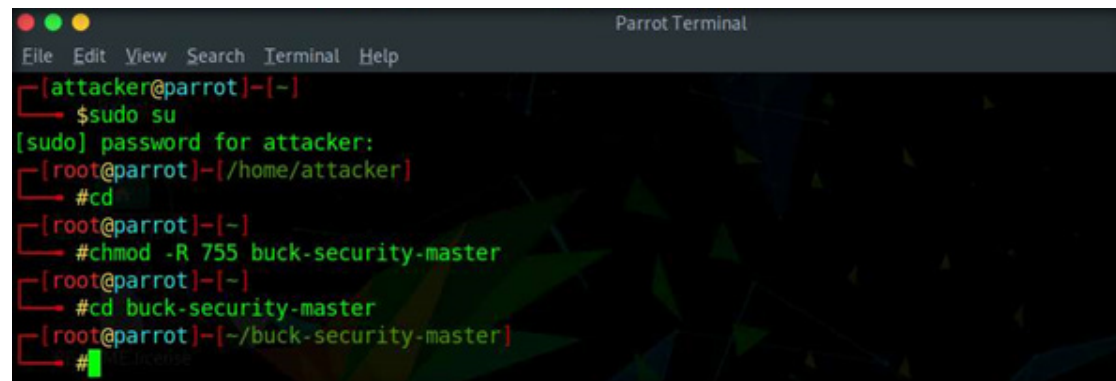
5. In the [sudo] password for attacker field, type toor as a password and press Enter.  
Note: The password that you type will not be visible.
6. Now, type cd and press Enter to jump to the root directory.
7. Type chmod -R 755 buck-security-master and press Enter to give adequate permissions to the tool folder.



```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
└─# cd
[root@parrot]-[-]
└─# chmod -R 755 buck-security-master
[root@parrot]-[-]
└─#
```

# EXERCISE 1: CONDUCT SECURITY CHECKS USING BUCK-SECURITY ON LINUX

8. Type `cd buck-security-master` and press Enter.



```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
└─# cd
[root@parrot]-[~]
└─# chmod -R 755 buck-security-master
[root@parrot]-[~]
└─# cd buck-security-master
[root@parrot]-[~/buck-security-master]
└─#
```

EXERCISE 1:  
CONDUCT SECURITY  
CHECKS USING  
BUCK-SECURITY ON  
LINUX



9. Type `./buck-security` and press Enter. This command will run a security scan on the Linux machine and check for vulnerabilities in the machine.

10. The result displays the issues found in the security measures with security WARNING messages, as shown in the screenshot below.

```

Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ] - [ ~/buck-security-master ]
[ # ./buck-security

#####
# buck-security 0.7 #
#####

We will run 13 security checks now.
This may take a while...

[1] CHECK checksum: Checksums of system programs [ WARNING ]
The security test encountered the following error during execution.
Couldn't read ./checksums.gpg: No such file or directory
Command was: a perl script, too long to display

[2] CHECK emptypasswd: Users with empty password [ WARNING ]
The security test encountered the following error during execution.
Password file /root/buck-security-master/etc/passwd does not exist.
Command was: a perl script, too long to display

[3] CHECK firewall: Check firewall policies [ WARNING ]
The security test discovered a possible insecurity.
The following iptables policies are set to ACCEPT.
#####
    
```

EXERCISE 1:  
CONDUCT SECURITY  
CHECKS USING  
BUCK-SECURITY ON  
LINUX

11. Scroll-down to view the complete result. Observe the section [3] CHECK firewall: Check firewall policies. This section shows the complete settings of the Firewall in the Linux machine. Similarly, observe other security warning messages along with the corresponding security issues.

EXERCISE 1:  
CONDUCT SECURITY  
CHECKS USING  
BUCK-SECURITY ON  
LINUX

```

Parrot Terminal
File Edit View Search Terminal Help
Command was: a perl script, too long to display

[2] CHECK emptypasswd: Users with empty password [ WARNING ]
The security test encountered the following error during execution.
Password file /root/buck-security-master/etc/passwd does not exist.
Command was: a perl script, too long to display

[3] CHECK firewall: Check firewall policies [ WARNING ]
The security test discovered a possible insecurity.
The following iptables policies are set to ACCEPT.
#####
FORWARD:ACCEPT
INPUT:ACCEPT
OUTPUT:ACCEPT
Command was: a perl script, too long to display

[4] CHECK packages_problematic: Search problematic packages [ WARNING ]
The security test discovered a possible insecurity.
The following packages are installed.
#####
dsniff
hping3
john
nikto
nmap
python-scapy
tshark
    
```

12. These security issues and vulnerabilities can further be analyzed and mitigated to enhance the overall security infrastructure of an organization's network.
13. This concludes the demonstration showing how to conduct security checks on Linux system.
14. Close all open windows.
15. Turn off the Attacker Machine-2 virtual machine.

# EXERCISE 1: CONDUCT SECURITY CHECKS USING BUCK-SECURITY ON LINUX

## EXERCISE 2: ANALYSIS AND VALIDATION OF MALWARE INCIDENT

The analysis of compromised systems, network, databases, files and other devices is important to validate a security incident.

### LAB SCENARIO

Modern attackers use sophisticated malware techniques as cyber weapons to steal sensitive data. Malwares such as viruses, trojans, worms, spyware, and rootkits allow an attacker to breach security defences and subsequently attack the target systems. Malware can cause the target an individual, a group of people, or an organization—to suffer intellectual and financial losses. Moreover, the malware spreads from one system to another with ease and stealth.

Thus, security professionals must find and fix existing infections and thwart future attacks. This can be achieved by performing malware analysis.

### OBJECTIVE

This lab demonstrates how to analyze and validate a malware incident, through the following:

- Analyzing viruses using an open-source malware analysis tool called VirusTotal
- Identifying suspicious file through packaging and obfuscation methods using PE

### OVERVIEW OF INCIDENT ANALYSIS AND VALIDATION

Incident responders must analyze the indicators of a reported issue to verify whether it is an information security incident or an error in the hardware or software components. The IH&R team should ideally evaluate each indicator to determine whether the incident legitimate. They must find the different sources of indicators, examine the security solutions, verify the system and device logs, and identify the incident and its vectors. An accurate, indicator does not necessarily mean that an incident has occurred. All incidents cannot be security incidents; some incidents such as web server crash and the modification of sensitive files could have been caused by human errors. The incident analysis will help determine whether the IH&R team needs to handle the incident, register the issue and take further action, or pass it to other teams for processing.

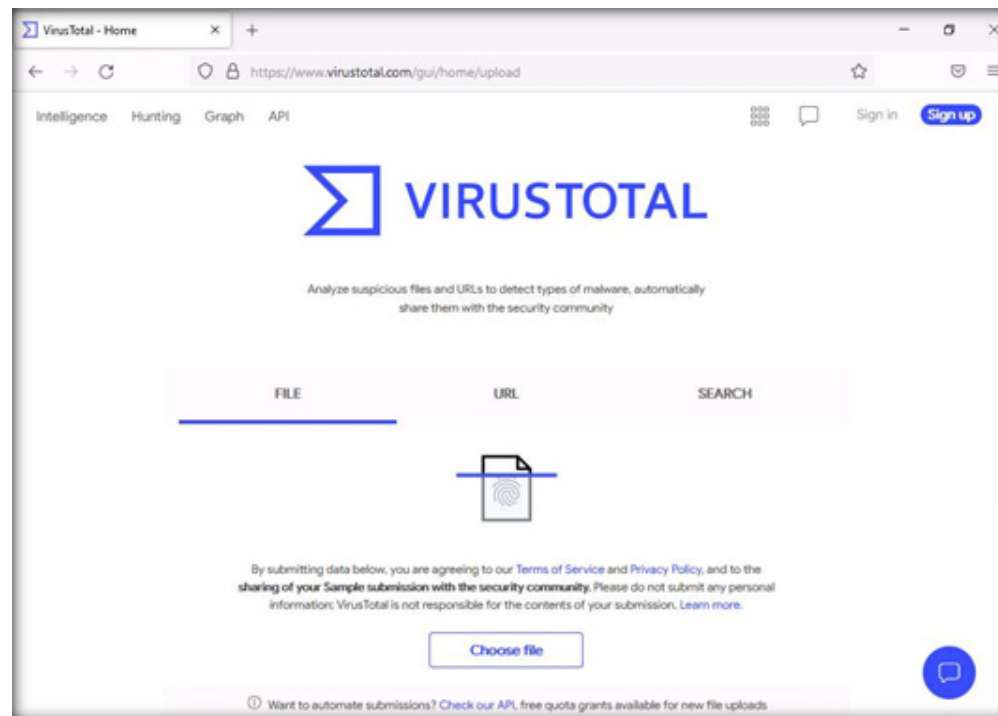
Note: Ensure that the PfSense Firewall virtual machine is running.

1. Turn on the Admin Machine-1 virtual machine.

2. Log in with the credentials Admin and admin@123.

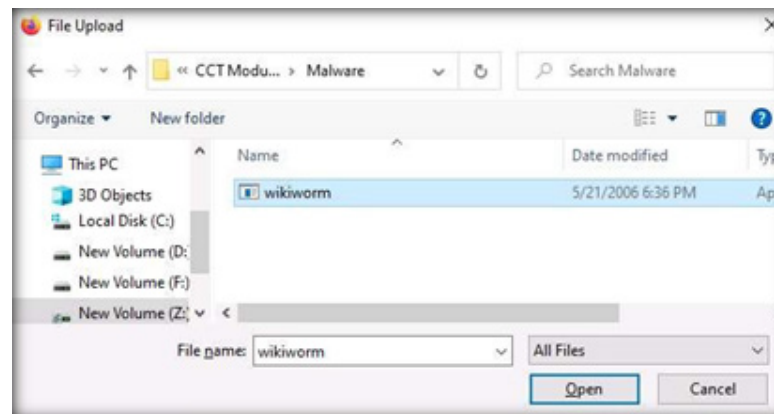
Note: If Networks prompt appears once you have logged into the machine, click Yes.

3. Open any web browser (in this lab task Mozilla Firefox) and place the mouse cursor on address field then, type `https://www.virustotal.com/#/home/upload` and press Enter. The VirusTotal home page will appear. Click Choose file.



EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

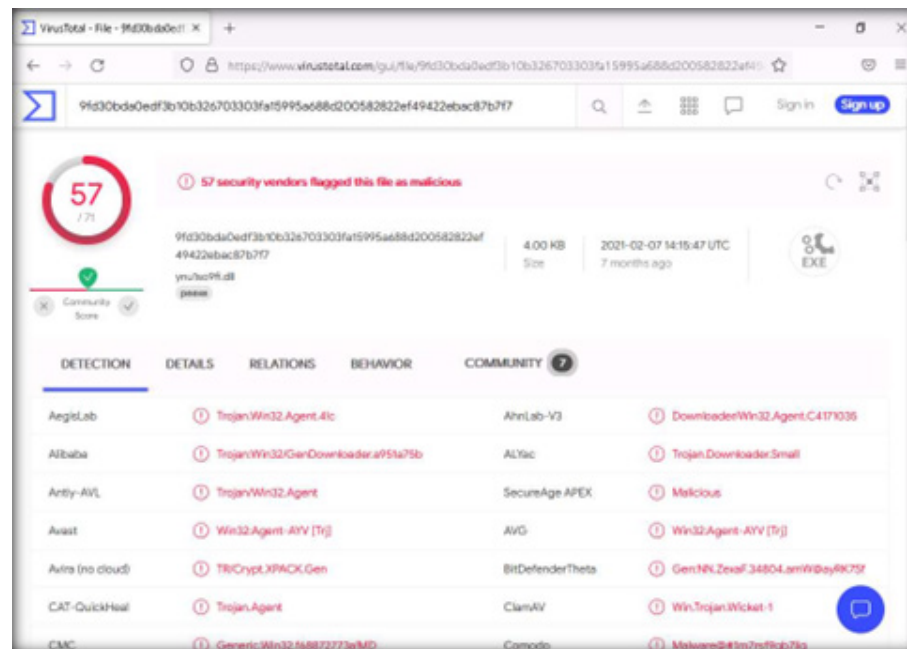
4. When the Open window appears, navigate to Z:\CCT-Tools\CCT Module 19 Incident Response\Malware, select the wikiworm.exe application, and click Open.



EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

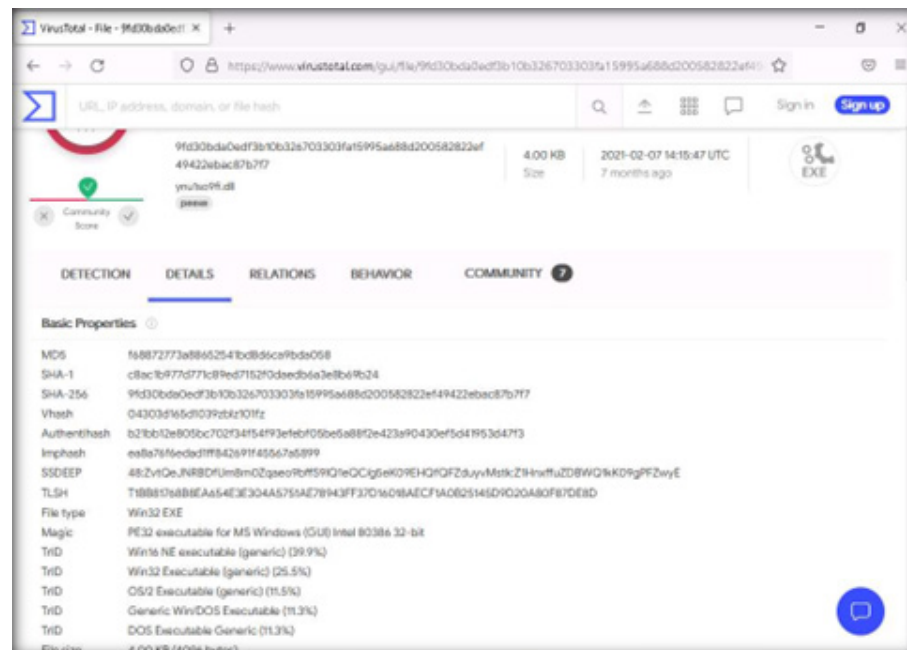
5. VirusTotal will automatically start computing the hashes and other signatures with well-known threat indicators from various sources and subsequently produce a malware infection score. View the result of the malware analysis of wikiworm.exe.

6. The VirusTotal score is 57/71 and all the results are shown in detail under the Detection tab.  
Note: The VirusTotal score may vary when you perform this lab.



EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

7. Click on the Details tab to extract more details about IoCs of the malware, such as MD5, SHA-1, Authentihash, Imphash, SSDeep, TRiD and File size.

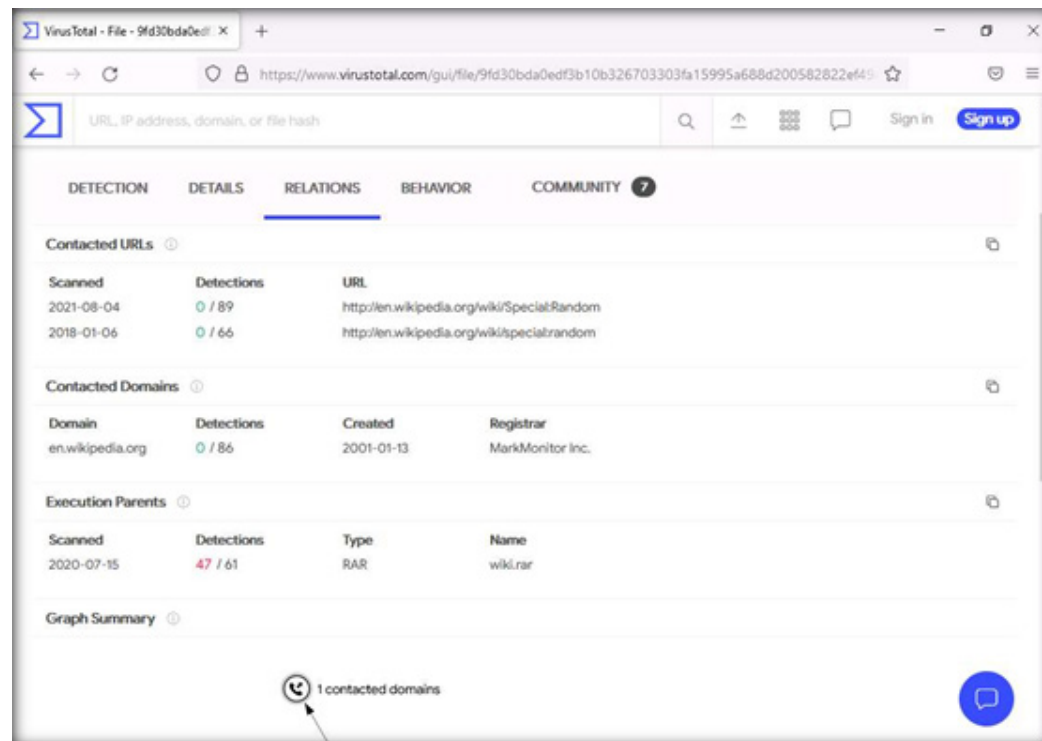


EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

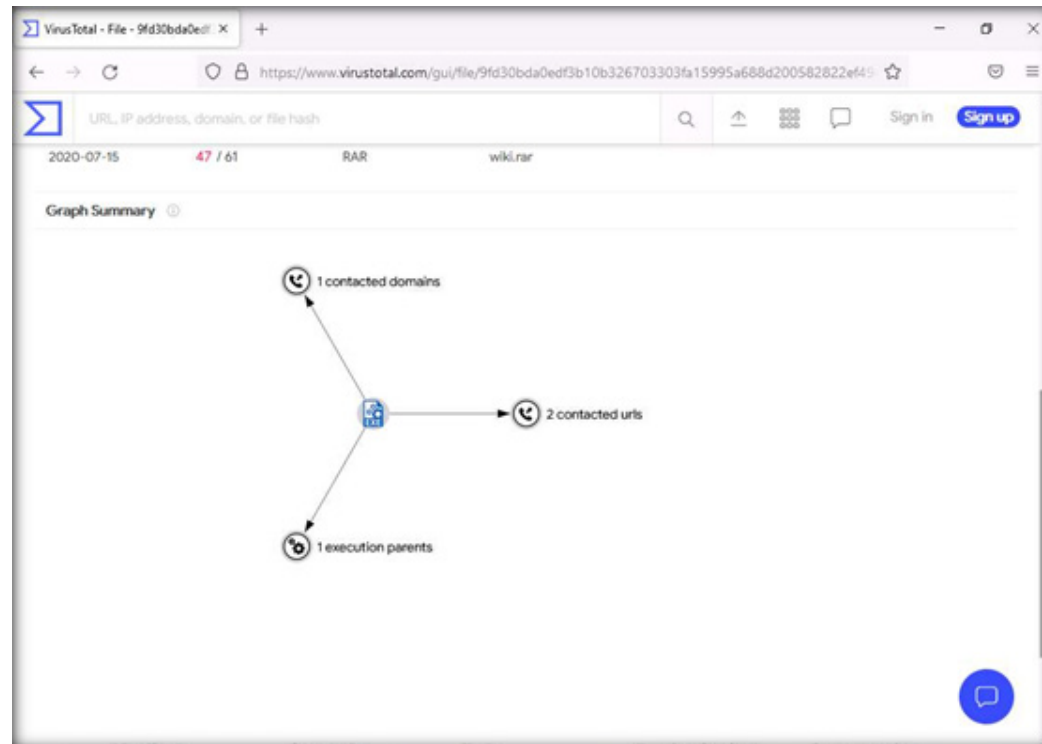


8. Click on the Relations tab to view the relations of the malware using Contact URLs, Contacted Domains, Execution Parents and Graph Summary.

EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

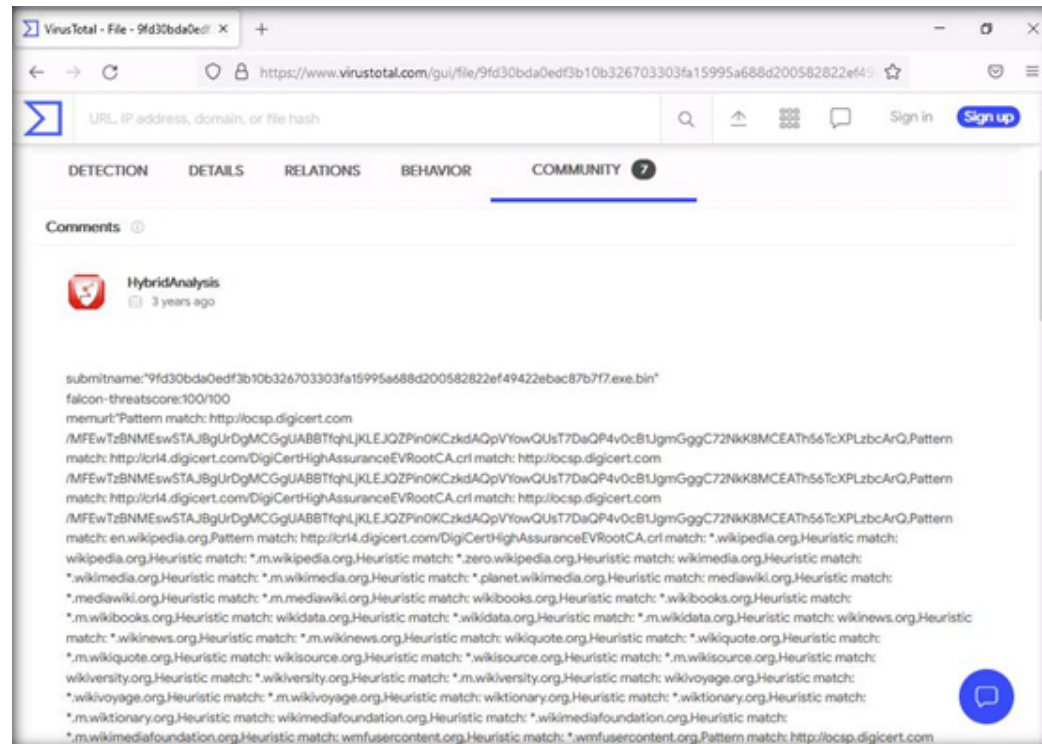


EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

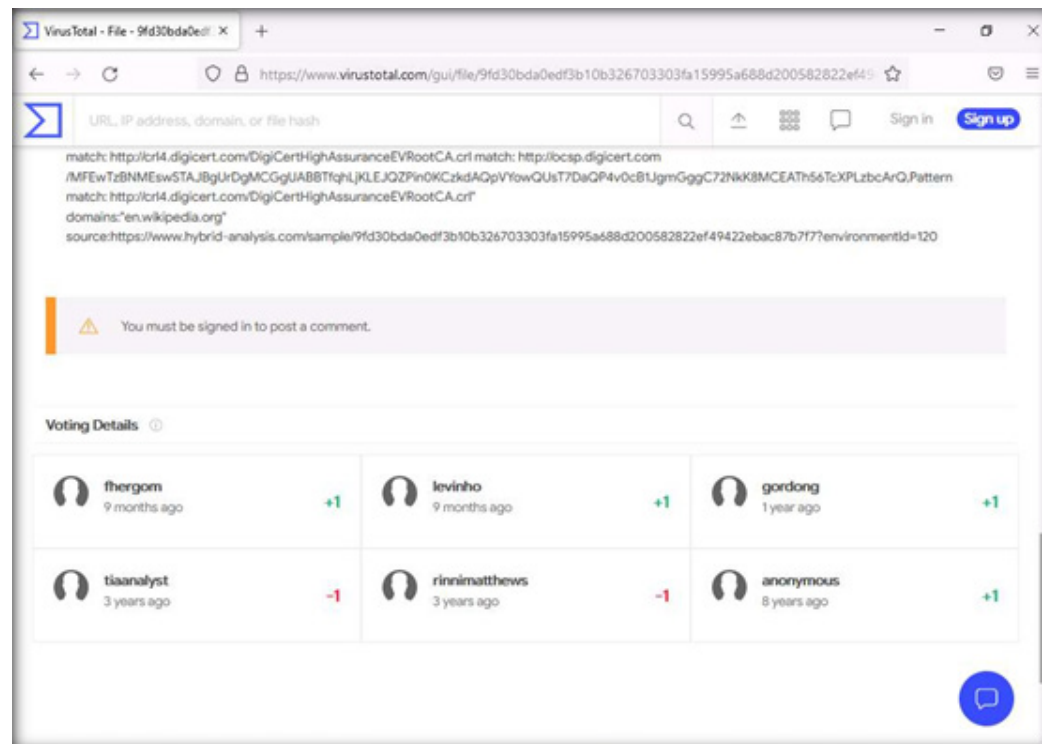


9. Click on the Community tab to view details such as HybridAnalysis and number of votes by the community members under the Voting Details section.

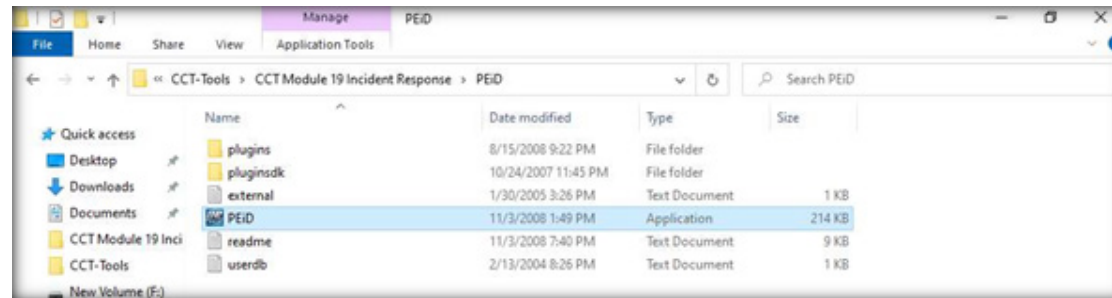
EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT




EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

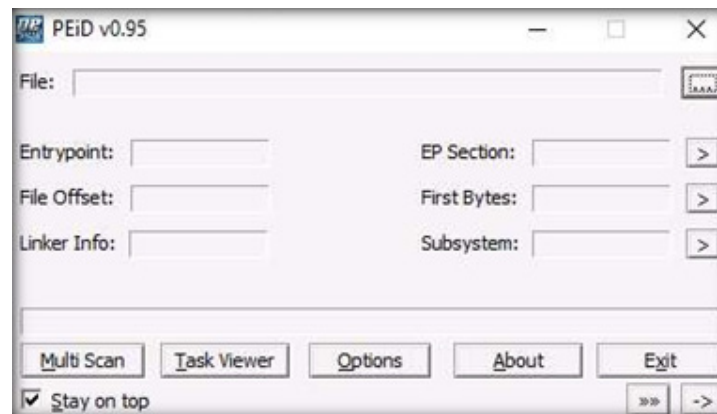


10. This concludes the demonstration showing how to analyze malware using VirusTotal.
11. Close the browser window.
12. Now, we will analyze a suspicious file created through packaging and obfuscation methods using PEid.
13. Navigate to Z:\CCT-Tools\CCT Module 19 Incident Response\PEid and double-click PEid.exe.



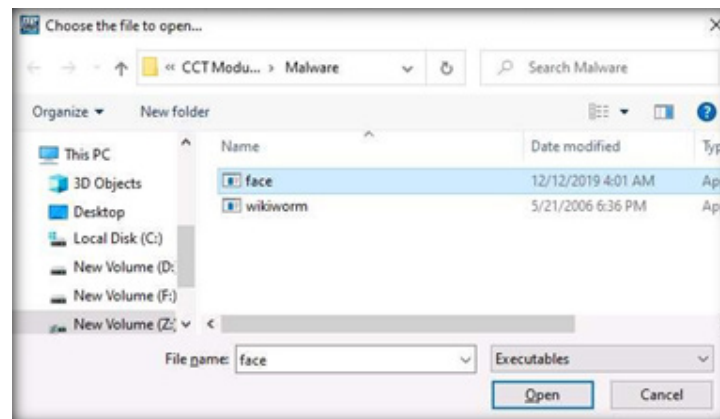
EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

14. The PEiD main window appears. Click the Browse button (  ) to upload a malicious file for analysis.



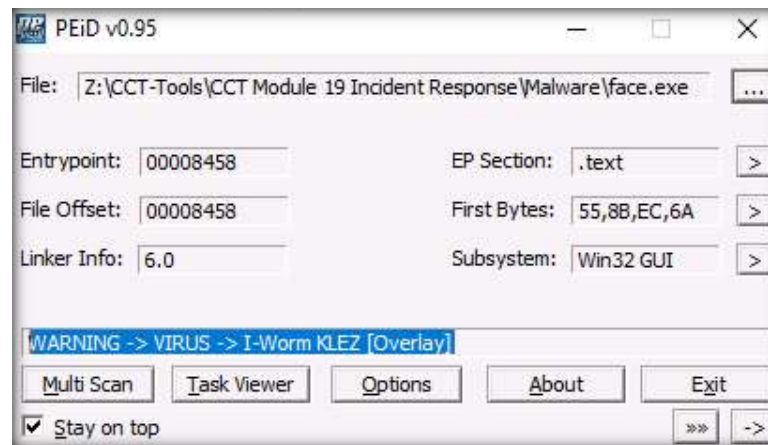
EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

15. The Choose the file to open window appears; navigate to Z:\CCT-Tools\CCT Module 19 Incident Response\Malware, select the face.exe application, and click Open.



EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

16. As soon as you click Open, PEiD analyzes the file and provides information, as shown in the screenshot below.



EXERCISE 2:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT



17. Close all windows once the analysis is complete.
18. This concludes the demonstration showing how to identify malicious file using PEiD.
19. Close all open windows.
20. Turn off the Admin Machine-1 virtual machine.

## EXERCISE 2: ANALYSIS AND VALIDATION OF MALWARE INCIDENT

## EXERCISE 3: IMPLEMENT POLICIES USING GROUP POLICY MANAGEMENT CONSOLE

The Group Policy Management Console (GPMC) is a scriptable interface to manage Group Policy.

### LAB SCENARIO

Preparation is the first and most important phase in the incident handling process as it enables the organization to establish an efficient incident response process. These preparation steps empower the incident handling and response (IH&R) teams to detect security incident at an early stage, before being notified about the incident by an external entity.

In this phase, security professionals need to define the mission, vision, and scope of IH&R; obtain management approvals and funding; develop and implement security policies; build an IR team; gather the systems, hardware, and software tools required for IR; prioritize assets and services; and create a plan for smooth communication during an incident.

This preparation helps security professionals to manage incidents more quickly and efficiently. A security professional must understand how to develop and implement various security policies to strengthen defences.

### OBJECTIVE

This lab will demonstrate how to implement policies using the Group Policy Management Console (GPMC).

### OVERVIEW OF GROUP POLICY MANAGEMENT CONSOLE

Group Policy Preferences provide more than twenty Group Policy extensions that expand the range of configurable preference settings in a Group Policy Object (GPO). Group Policy enables the management of drive mappings, registry settings, local users and groups, services, files, and folders without the need to learn a scripting language.

Note: Ensure that the PfSense Firewall virtual machine is running.

1. Turn on the AD Domain Controller virtual machine.

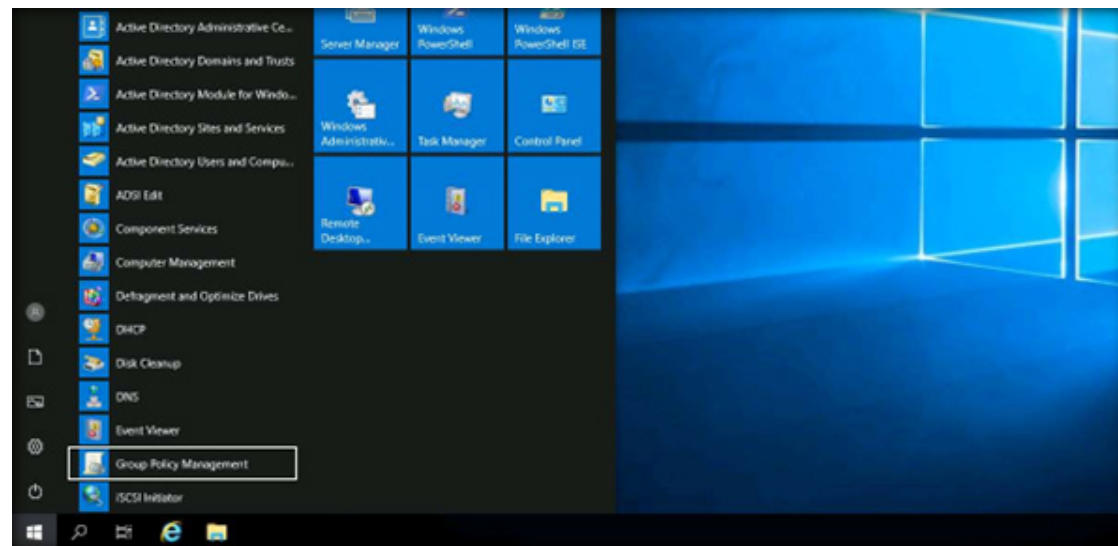
2. Log in with the credentials CCT\Administrator and admin@123.

Note: The network screen appears, click Yes.

Note: If a Shutdown Event Tracker window appears, click Cancel.

3. To launch Group Policy Management, click the Start icon, and then navigate to Windows Administrative Tools → Group Policy Management.

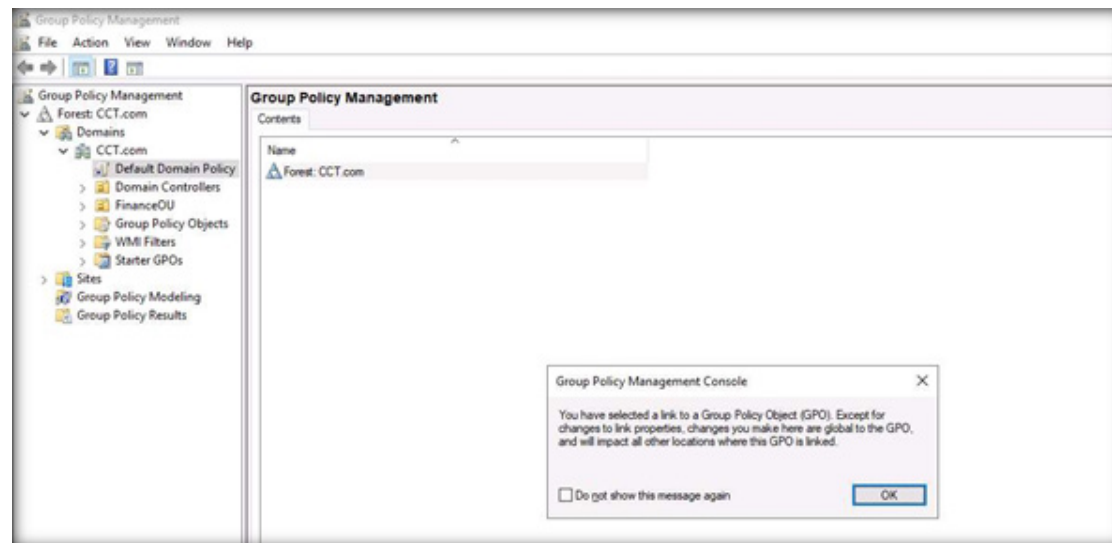
Note: Alternatively, launch the Run window, type gpmmc and press Enter to launch Group Policy Management.



EXERCISE 3:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

4. The main window Group Policy Management appears. From the left-pane, expand the Forest: CCT.COM node, Domains node and CCT.com domain node.

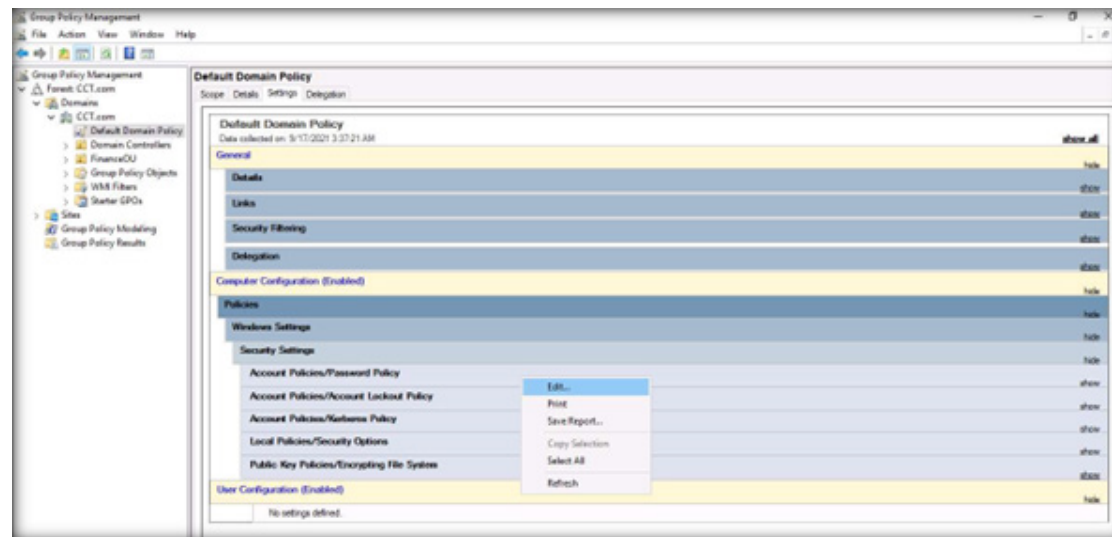
5. Under CCT.com, select the Default Domain Policy profile from the left-pane. A Group Policy Management Console pop-up appears. Click OK.



EXERCISE 3:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

6. Default Domain Policy appears in the right-pane. Click Settings tab.

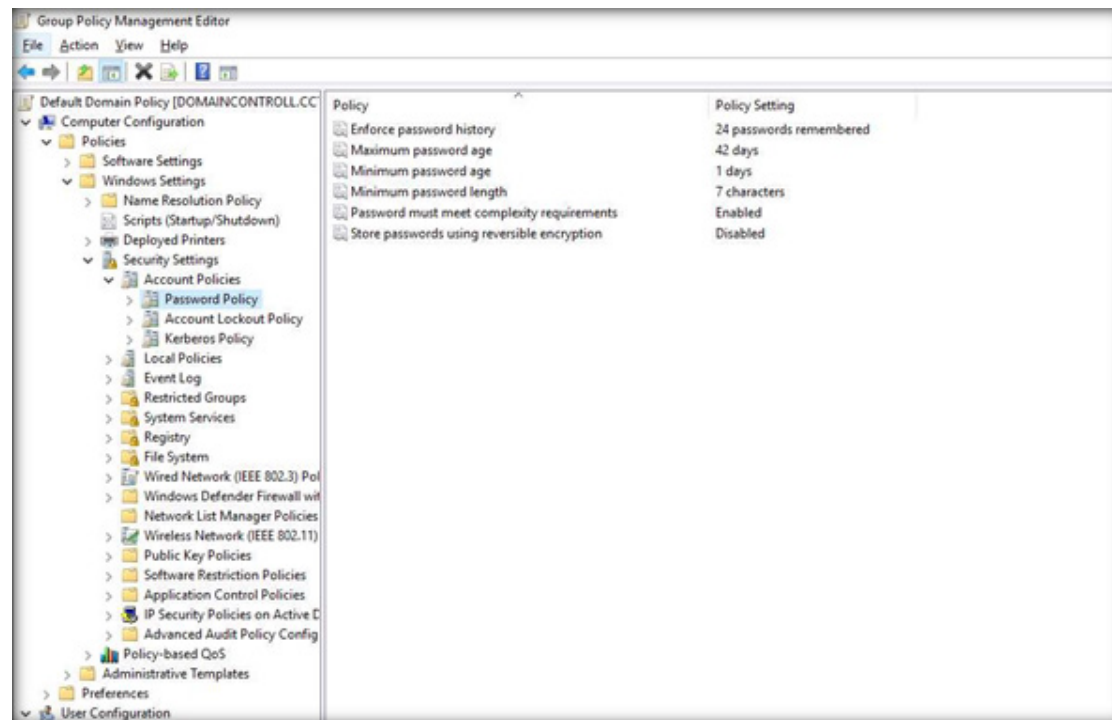
7. Under the Computer Configuration section, click to expand the Security Settings, then right-click Account Policies/Password Policy and click Edit... from the context menu. To configure the password policies for domain users.



EXERCISE 3:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

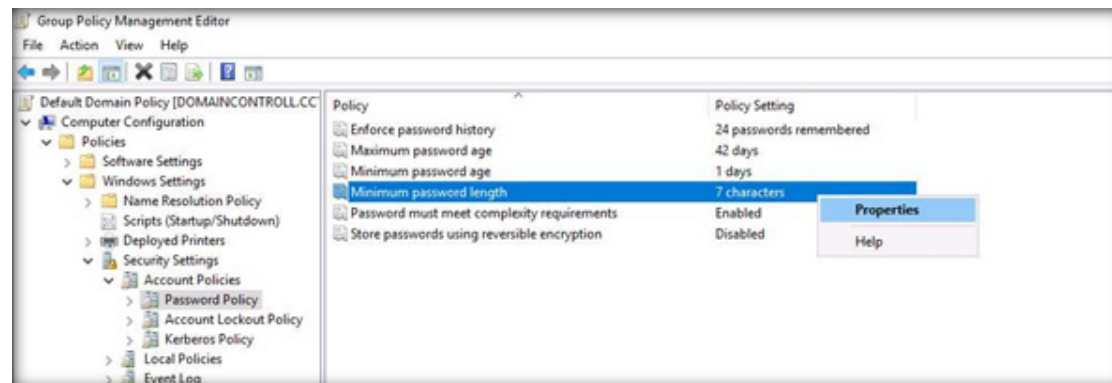
8. In this lab, we will set password policies for the domain users. The Group Policy Management Editor window appears. In the left-pane, navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy.

9. In the right-pane, Policy and Policy Setting appears, as shown in the screenshot below.



EXERCISE 3:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

10. Set password policies according to the organization’s policy. To edit the policy settings, right-click any policy (here, Minimum password length), and click Properties from the context menu.



EXERCISE 3:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT

11. The window appears showing properties of the selected policy; policy settings can be defined under the Security Policy Setting tab. In the Password must be at least field, increase the minimum number of characters to 15.

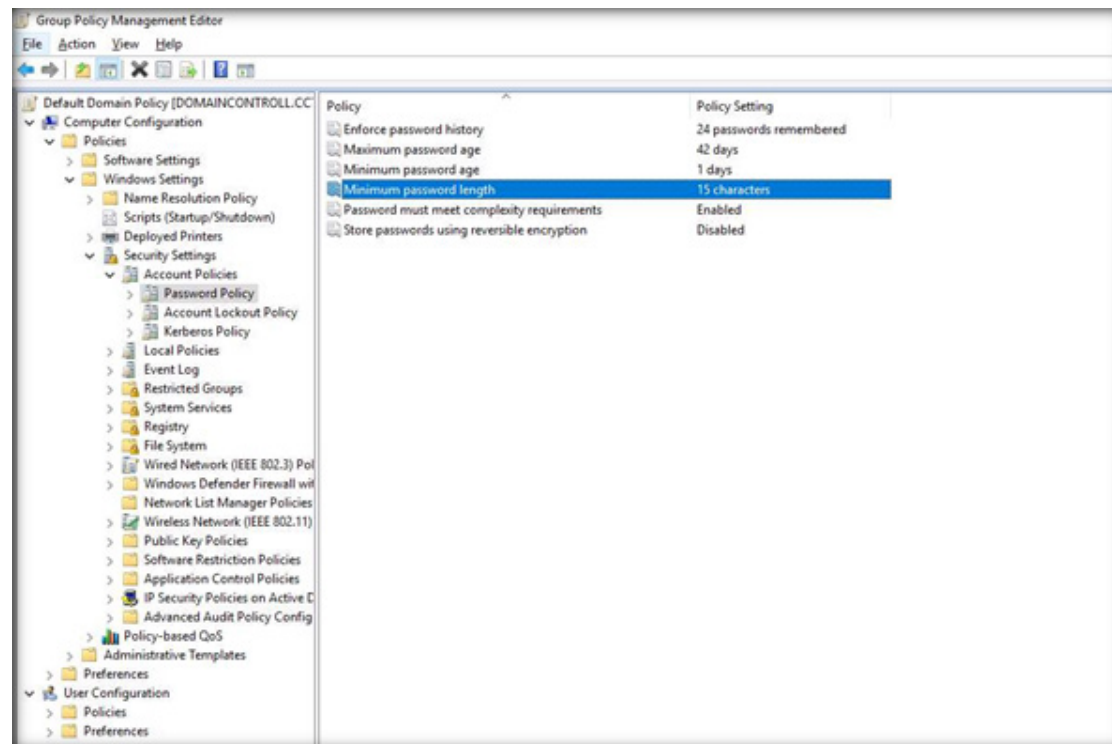


EXERCISE 3:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT



12. The Explain tab has a brief description of the selected policy; read the explanation and edit the policy, according to the organization's policy.
13. Click the OK button to close the policy properties window.
14. Observe that the selected policy has been configured. Similarly, other password policies can be configured according to the organization's policies.

EXERCISE 3:  
ANALYSIS AND  
VALIDATION OF  
MALWARE INCIDENT



15. This concludes the demonstration of showing how to implement policies using the Group Policy Management Console (GPMC).
16. Close all open windows.
17. Turn off AD Domain Controller and PfSense Firewall virtual machines.

## EXERCISE 3: ANALYSIS AND VALIDATION OF MALWARE INCIDENT



# EC-Council