





CERTIFIED CYBERSECURITY TECHNICIAN

Copyrights @ 2022 EC-Council International Ltd.







Chapter 19: Incident Response

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





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:



Conduct Security Checks using buck-security on Linux



Analysis and Validation of Malware Incident



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 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.





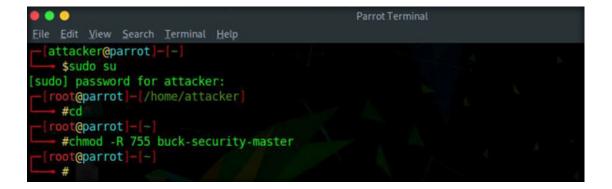


5. In the [sudo] password for attacker field, type toor as a password and press Enter. Note: The password that you type will not be visible.

6. Now, type cd and press Enter to jump to the root directory.

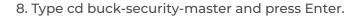
7. Type chmod -R 755 buck-security-master and press Enter to give adequate permissions to the tool folder.

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

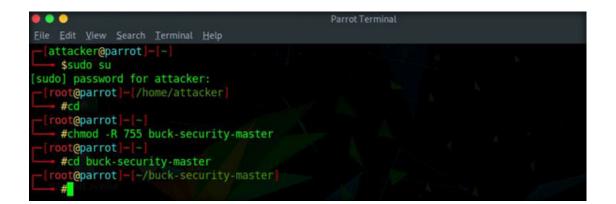








EXERCISE 1: CONDUCT SECURITY CHECKS USING BUCK-SECURITY ON INUX



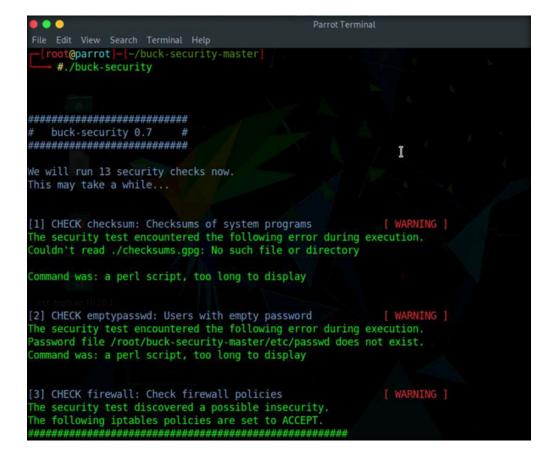




9. Type ./buck-security and press Enter. This command will run a security scan on the Linux machine and check for vulnerabilities in the machine.

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

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 JINUX

	Parrot Terminal
File Edit View Search Terminal Help	
Command was: a perl script, too long to disp	olay
[2] CHECK emptypasswd: Users with empty pass The security test encountered the following Password file /root/buck-security-master/etc Command was: a perl script, too long to disp	error during execution. c/passwd does not exist.
T	
[3] CHECK firewall: Check firewall policies The security test discovered a possible inse The following iptables policies are set to a ####################################	ACCEPT.
Command was: a perl script, too long to dis	play
[4] CHECK packages_problematic: Search prob The security test discovered a possible inso The following packages are installed.	
######################################	******
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 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.

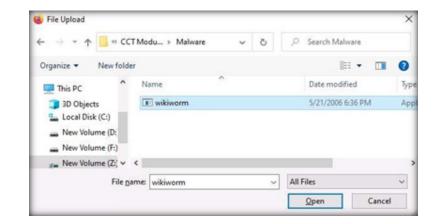
3. Open any web browser (in this lab task Mozilla Firefox) and place the mouse cursor on address field then, type https://www.virustotal. com/#/home/upload and press Enter. The VirusTotal home page will appear. Click Choose file.

VirusTotal - Home	×	+				-	0	×
$\leftarrow \ \rightarrow \ \mathbf{C}$	0 6	https://www.virustotal.c	com/gui/home/upload				\odot	=
Intelligence Hunting	Grag	ph API		000 000 000	\Box	Sign in	Signup	Ĩ
		_	VIRUSTC ious files and URLs to detect types of mal share them with the security communi	ware, automatically				
		FILE	URL	SEARCH				
		sharing of your Sample subr	you are agreeing to our Terms of Service mission with the security community. Pl is not responsible for the contents of you Choose file	lease do not submit any personal				
		Want to automate submit of the submit of	missions? Check our API, free quota gran	ts available for new file uploads			0	





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.









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.



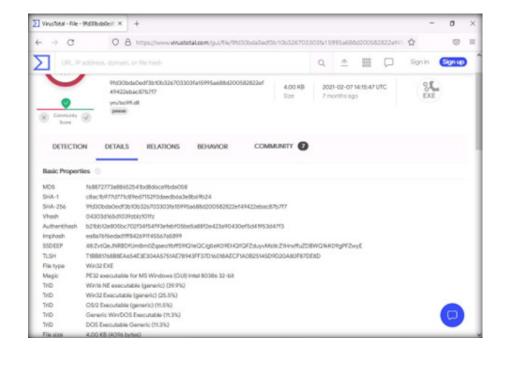
VirusTotal - File - 91d00	dsöeri × +				-	٥
← → C	O A https://www.winustetal.com/gui/file/91d30bda0e	#3610632670330	35a15995a688	4200582822	ef45 🟠	0
9fd30bda0e	df3b10b326703303fa15995a688d200582822ef49422ebac87	b717	Q. 🖄	\$\$\$ F) Signin	Signup
57	① 57 security vendors flagged this file as multicious					e X
S Connectly @	9fc30bda0ed73br0b326703303fe15995a688d200582822ef 49422ebac87b2f7 ym/se9fi.dll jeana	4.00 KB Size	2021-02-07 7 months ag		SK EXE	•
DETECTION	DETAILS RELATIONS BEHAVIOR COM		0	Proverbander	Wn32 Agent C41	790.94
Negocou	O milanmazagenan	Perilag-13	0	Downooder	in scrigenceri	10.00
Alibaba	Trojan/Wir32/GenDownkoeder.a/95ta75b	ALYSIC	0	Trojan Downi	oader.Small	
Albaba Antiy-AVL	Trojan/Wn32/GenDownloader.a//51a75b Trojan/Wn32/GenDownloader.a//51a75b	ALYac SecureAge APE		Trojan Downi Malicious	oeder.Smell	
			0			
Anthy-AVL	Trojan/Wini2.Agent	SecureAge APE	0	Melicious Win32Agent		y#86757
Antiy-AVL Awast	Trojan/Win32.Agent Win32.Agent-AlfV [Trj]	SecureAge APE AVG	(() () () ()	Melicious Win32Agent	-AVV (Trj) # 34804.amWibe	×××757





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: NNALYSIS AND MALION 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.

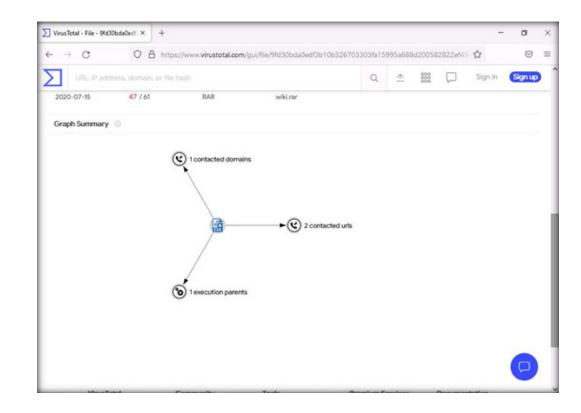
EXERCISE 2: ANALYSIS AND MALIDATION OF MALWARE INCIDENT

URL, IP addr	ess, domain, or fil				Q	<u>_</u>	335	Sign in	Signu
-					-				
DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNIT	Y 🕖				
Contacted URLs									0
Scanned	Detections	URL							
2021-08-04	0/89	http://	en.wikipedia.org/w	viki/Special:Random					
2018-01-06	0/66	http://	en.wikipedia.org/v	/iki/specialtrandom					
Contacted Domai	ns 🛈								0
Domain	Detections	Creat	ed	Registrar					
en.wikipedia.org	0/86	2001-	01-13	MarkMonitor Inc.					
Execution Parents	• @								0
Scanned	Detections	Туре		Name					
2020-07-15	47 / 61	RAR		wiki.rar					
Graph Summary									





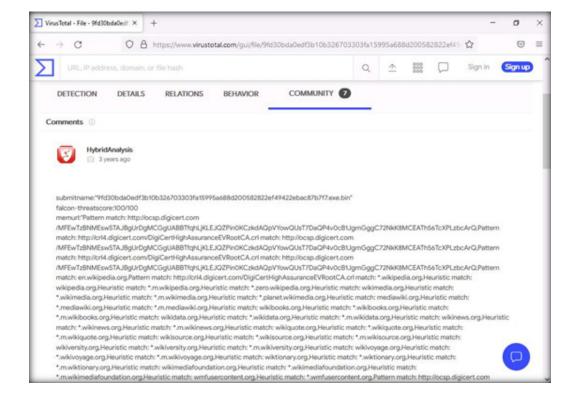






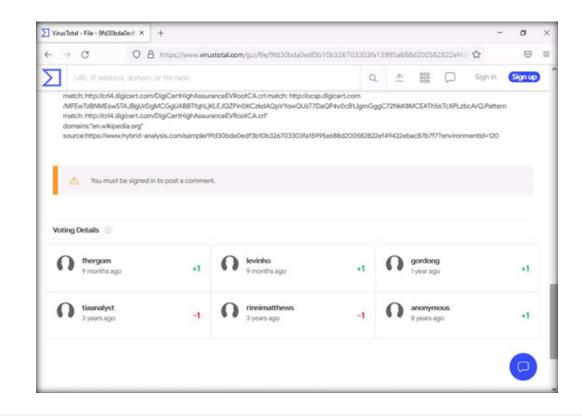


9. Click on the Community tab to view details such as HybridAnalysis and number of votes by the community members under the Voting Details section.













- 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.

1 🖸 📑 🖬 1	Manage	PEID			-	0	×
File Home Share	View Application Tools						~ (
← → ~ ↑ <mark>=</mark> « cc	T-Tools > CCT Module 19 Inciden	t Response > PEiD	~ Ö	,P Search PEiD			
	Name	Date modified	Type	Size			
A Quick access	plugins	8/15/2008 9:22 PM	File folder				
Desktop 🖈	pluginsdk	10/24/2007 11:45 PM	File folder				
Downloads x*	external	1/30/2005 3:26 PM	Text Document	1 KB			
🔁 Documents 🛷	PEID	11/3/2008 1:49 PM	Application	214 KB			
CCT Module 19 Inci	readme	11/3/2008 7:40 PM	Text Document	9 KB			
CCT-Tools	userdb	2/13/2004 8:26 PM	Text Document	1 KB			
New Volume (F:)							





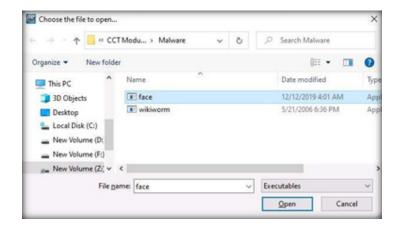
14. The PEiD main window appears. Click the Browse button (

File:		
Entrypoint:	EP Section:	
File Offset:	First Bytes:	[
Linker Info:	Subsystem:	[
Multi Scan Task Viewer	Options About	Exit
Stay on top		30.30





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.







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

Entrypoint:	00008458	EP Section:	.text	[
File Offset:	00008458	First Bytes:	55,88,EC,6A	
Linker Info:	6.0	Subsystem:	Win32 GUI	- [





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 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 gpmc.msc and press Enter to launch Group Policy Management.







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.

Group Policy Management A Forest CCT.com Comparing	Group Policy Management Contents		
 Bornains Bornains Default Domain Policy Default Domain Controllers FinanceOU Group Policy Objects Stater GPOs State Group Policy Medding Group Policy Results 	Name A Forest: CCT.com	Group Policy Management Console You have selected a link to a Group Policy Object (GPO). Except for changes to link properties, changes you make here are global to the GPO and will impact all other locations where the GPO is linked.	×
		Do got show this message again OK	







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.

File Action View Window H	*0		
🔶 🔶 🙇 📷 🖄 🖬 📾			
Group Palicy Management A forest CCL.com V A Domaine	Default Domain Policy Scope Details Settings Delegation		
gli CCLearn Gl Dafault Domain Policy S Domain Controllers	Data collected on 3/11/2021 3/37/21 AM		dor.d
 SinancaOU Group Policy Objects WM Fibers 	General Details		tak .
) 🤤 Starter GPOs	Loka		there are a second s
👸 Group Palicy Medaling 🚬 Group Palicy Results	Security Filtering Delegation		daa
	Computer Configuration (Enabled)	etan huk	
	Pulkies		-
	Windows Settings		habe a
	Security Settings		1.0
	Account Policies/Password Policy		
	Account Pulicies/Account Lackout Policy	Edit	stew
	Account Policies/Kerlsows Policy	Save Report.	and an and an
	Local Pulicies/Security Options	Copy Selection	den
	Public Key Policies/Encrypting File System	Select All	dan dan
	User Configuration (Enabled)	Retext	hale .
	No settings defined.		108





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.

Default Domain Policy [DOMAINCONTROLL.CC] Computer Configuration Schware Settings Software Settings Software Settings Software Settings Scripts (Startup/Shutdown) Seripts (Startup/Shutdown) Security Settings System Services Settings Windows Defender Firewall wit Windows Defender Firewall wit Wireless Network (IEEE 802.3) Policies Wireless Network (IEEE 802.11)	Policy Enforce password history Maximum password age Minimum password age Minimum password length Password must meet complexity requirements Store passwords using reversible encryption	Policy Setting 24 passwords remembered 42 days 1 days 7 characters Enabled Disabled





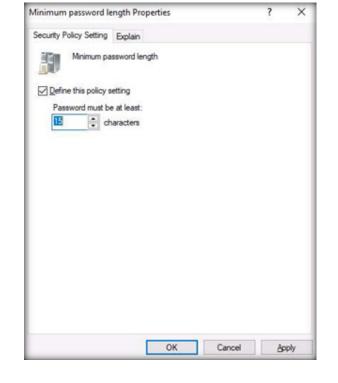
10. Set password policies according to the organization's policy. To edit the policy settings, right-click any policy (here, Minimum password length), and click Properties from the context menu.

Group Policy Management Editor			
File Action View Help			
🕶 🔿 🙍 📷 🗙 🗊 🐼 📓 🖬			
Default Domain Policy [DOMAINCONTROLL.CC Computer Configuration Dolicies Software Settings Windows Settings	Policy Enforce password history Enforce password bistory Maximum password age Minimum password age Minimum password Innoh	Policy Setting 24 passwords ren 42 days 1 days 7 characters	nembered
> Name Resolution Policy Scripts (Startup/Shutdown)	Password must meet complexity requirements Store passwords using reversible encryption	Enabled Disabled	Properties
 Imp Deployed Printers Security Settings Account Policies Password Policy Account Lockout Policy Kerberos Policy Local Policies Securit Loa 			Help





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.



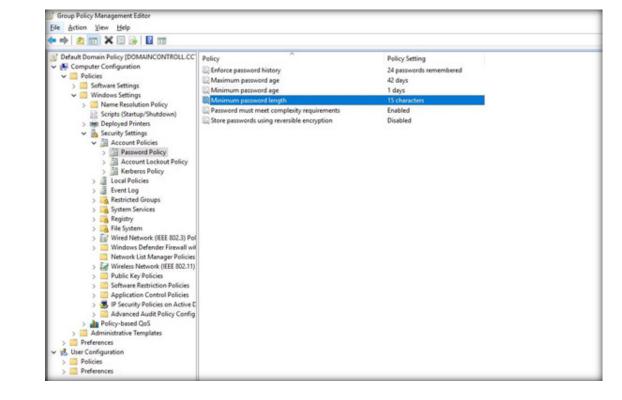




12. The Explain tab has a brief description of the selected policy; read the explanation and edit the policy, according to the organization's policy.

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.







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.

EC-Council