LETTER OF ENGAGEMENT

THREAT HUNTING PROFESSIONAL V2

eLearn Security
AN INE COMPANY

eLearnSecurity has been chosen by students in 140 countries in the world and by leading organizations such as:

hp Microsoft intel cisco AT&T verizon U.S. AIR FORCE pwc gemalto security to be free

I. EXAM CONFIGURATION AND TESTS

Before starting your Threat Hunting exam process make sure that you have read, understood and accepted the following eLearnSecurity certification terms and conditions, in full.

https://www.elearnsecurity.com/certification/ecthp/terms

Make also sure that your environment is properly configured. Once you are connected through the VPN please test your connection to the exam environment by pinging the following IP address:

172.16.85.103 (Scenario 1 Using Splunk)

172.16.85.104 (Scenario 2 Using Volatility)

172.16.85.102 (Scenario 3 Using ELK)

If you are able to ping all addresses you can start hunting!

II. SCOPE OF ENGAGEMENT

You are employed by the ELS organization to perform the following three (3) threat hunting activities:

Please refer to section "Deliverable" below on how to provide us with your findings.

HUNT 1: HUNT MAMABEAR (40 Points)

Study the provided Threat Intelligence report **eCTHPv2_MamaBear_Threat_Intelligence_Report.pdf** that describes a possible threat to ELS's Bank.

Start the eCTHPv2 Hunt 1 Scenario.

Connect to ELS Bank's Spunk at http://172.16.85.103:8000 (username: *admin*, password: *eLSHunter*)

ELS wants you to hunt for MamaBear activity in their bank (ELS Bank) using its Splunk-based SIEM.

IMPORTANT NOTES:

1. If you conclude that ELS Bank has been compromised by MamaBear, ELS would like to see how far the attackers went. This means that ELS would like to see evidence of MamaBear activity across the entire cyber kill chain (Initial Access, Attack Vectors/Payloads used, Enumeration, Lateral Movement, Privilege Escalation, Persistence, etc.) and across all endpoints/servers.
2. Leverage all available indexes and data sources. After logging into Splunk, you can find all available indexes at **Settings -> (Data) Indexes**.

HUNT 2: HUNT FOR .NET MALWARE IN MEMORY (30 Points)

Start the eCTHPv2 Hunt 2 Scenario.

Connect to `172.16.85.104` via **Remote Desktop** (username: *AdminELS*, password: *Nu3pmkfyX*, **port**: *65520*). A memory dump named **memdump.mem** can be found on the Desktop.

Volatility is installed and waiting for you inside the *Downloads* folder. Use the **Win10x64_18362** profile.

This memory dump file is related to an endpoint that ELS believes was infected by a .NET-based malware.

ELS wants you to hunt for .NET malware inside that memory dump file using Volatility.

IMPORTANT NOTE: You can use all installed tools on the machine for this hunt. Additionally, search online for .NET malware hunting resources.

HUNT 3: HUNT FOR SPECIFIC TTPS (30 Points)

Start the eCTHPv2 Hunt 3 Scenario.

Connect to **172.16.85.102** via **SSH** (username: *hunter*, password: *hunter*) and execute the following commands (it will take a few minutes to setup the environment):

```
cd /opt/elk-detection-lab
sudo ./elk-detection-lab.sh run
```

Once the environment is ready Kibana will be available via your browser at **http://172.16.85.102:5601**

ELS wants you to hunt for the below TTPs using its ELK-based SIEM

(TXXX is the respective MITRE ATT&CK technique number):

1. Timestomping MACE attributes (T1099) (**timeline between 01/04/2019 and 15/05/2019**)
2. Meterpreter Migrate command from untrusted process to a trusted one (explorer.exe) (T1055)
3. Process Creation through WMI (T1021) (**timeline between 01/04/2019 and 01/05/2019**)
4. MSSQL xp_cmdshell execution
5. Harvesting browser saved credentials (**Google Chrome**) (T1081)
6. Privilege escalation through RottenPotato (T1134) (**at 26.05.2019**)

III. EXAM OBJECTIVES

Please note that you are required to perform a thorough threat hunt utilizing all provided data and to report any threat identified and any threat identification technique that you used.

Your goal is to successfully perform all the threat hunting activities that **ELS** required.

The necessary but insufficient condition to pass the exam is:

- Gather a minimum of **75** points

A table report for the threat hunts must be produced that includes your findings.

NOTE: Any threat detection method used should be described in a step by step manner and accompanied by technical details (such as SIEM queries, Volatility commands, etc.). If there is not enough space on the table report, use appendixes.

Please document everything into a single PDF document.

IV. DELIVERABLE

The required table report should have the following format:

Hunt 1	
Task	**Findings**
Hunt N	
Task	**Findings**

EXAMPLE:

Hunt 1	
Task	**Answer/Finding**
ELS wants you to hunt for MamaBear activity in their bank (ELS Bank) using its Splunk-based SIEM.	After hunting for MamaBear activity, I concluded that ELS Bank has been breached by the abovementioned group. Initial access was gained through X (append Splunk query and screenshot). Leveraging the Y datasource I also noticed lateral movement through Z (append Splunk query,screenshot and the related endpoints/servers)…

V. RECOMMENDED TOOLS

You are free to use any of the installed tools on the hunting machines:

- ELK
- Splunk
- Volatility
- PowerShell
- Command line tools (check the *Path* variable to find which ones are available through the terminal)

Please note that you will need the OpenVPN client in order to connect to the exam environment.

VI. HINTS FOR THE BEST OUTCOME

Keep track of all of your actions, commands, findings, etc. while you perform your hunts.

Mind mapping is your friend!

Dive into all the available functionality of the tools covered in the course!!!

Quickly go through their documentation/wiki pages and available plugins to understand their full potential.

GOOD LUCK!