LETTER OF ENGAGEMENT

CERTIFIED INCIDENT RESPONDER

eLearnSecurity
Forging security professionals

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

- **Exam configuration and Tests**

Before starting your Incident Response 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/ecir/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 addresses:

172.16.157.100 (SPLUNK)

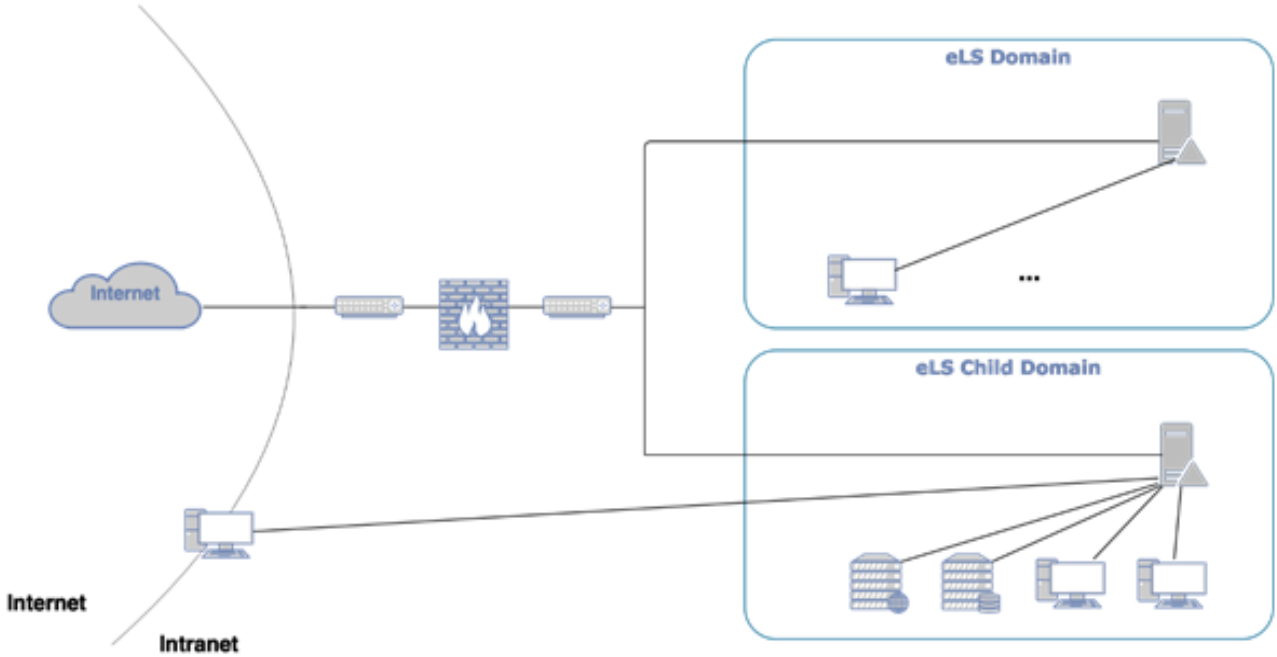
172.16.157.101 (ELK)

If you are able to ping both IP addresses, you can start your Incident Response activities.

- **Scope of engagement**

The eCIR exam consists of two **distinct** Incident Response scenarios.

Scenario 1: eLS Breach (60 points)



Above you can see the environment of the eLS organization. Two domains exist **ELS-CHILD** (child domain) and **ELS** (parent domain). Subsequently there are two Domain Controllers, **child-dc01** for **ELS-CHILD** and **lab-dc01** for **ELS**.

eLS is using Splunk as a SIEM solution.

You can log into Splunk (http://172.16.157.100:8000) using the credentials: admin/els@nalyst

eLS has only one internet-exposed endpoint, **win10-server. win10-server** belongs to the **ELS-CHILD** domain.

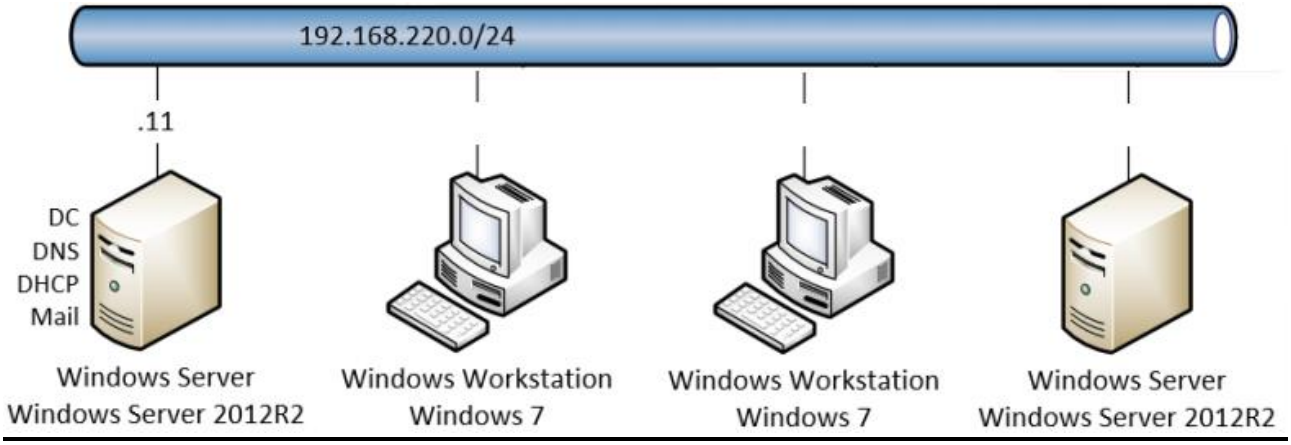
win10-server has been compromised.

Log into Splunk and identify every attacker activity. Specifically, you are required to identify:

- How initial foothold was gained
- How many hosts were accessed/compromised by the attacker
- Whether the attacker managed to access/compromise the parent domain's Domain Controller
- **Technical details** about the attack's lifecycle, such as attack vector(s)/payloads used, information gathering activities, scanning activities, exploitation activities, post-exploitation activities (including privilege escalation, lateral movement, forged Kerberos tickets, persistence etc.)

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

Scenario 2: TESTDOMAIN Breach (**40 Points**)



Above you can see the TESTDOMAIN environment. **W2012r2-DC01** is TESTDOMAIN's Domain Controller.

TESTDOMAIN is using ELK as a SIEM solution.

You can log into ELK (http://172.16.157.101:5601) without credentials

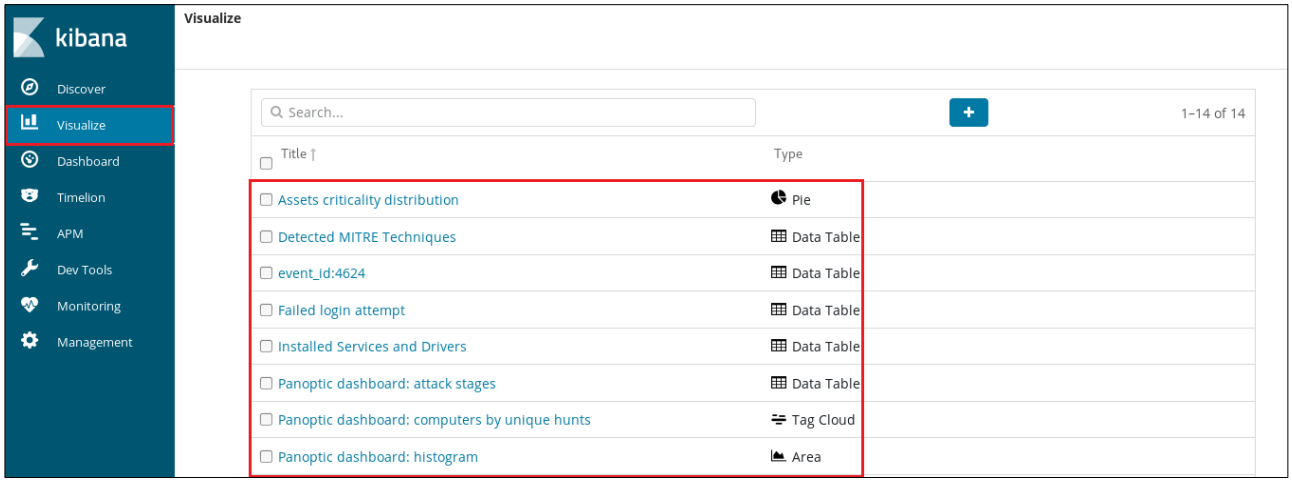
The **VICTIM** endpoint (192.168.220.100) has been compromised.

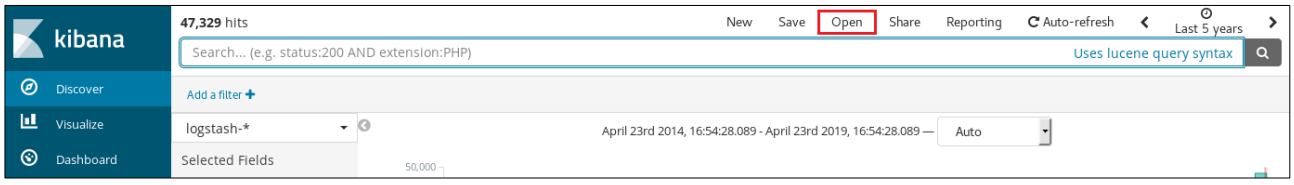
Log into ELK and identify every attacker activity. Specifically, you are required to identify:

- How initial foothold was gained
- How many hosts were accessed/compromised by the attacker
- Whether the attacker managed to access/compromise the Domain Controller
- **Technical details** about the attack's lifecycle, such as attack vector(s)/payloads used, information gathering activities, scanning activities, exploitation activities, post-exploitation

activities (including privilege escalation, lateral movement, forged Kerberos tickets, persistence etc.)

A dashboard, various visualizations and various saved searches are provided to help you in your Incident Response activities (not all will be useful).





In addition, you will find a PCAP file named **scenario2-traffic-capture.pcap** inside the letter of engagement ZIP file that contains traffic captured while the attack was taking place.

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

- **Exam objectives**

Please note that you are required to perform comprehensive Incident Response activities utilizing all the provided data and to report any attacker activity you identified and any detection technique that you used.

Your goal is to successfully respond to both scenarios' incidents.

The necessary but insufficient condition to pass the exam is:

Gather a minimum of **70** points.

A table report for the Incident Response activities must be produced that includes your findings.

> **Note**: Any detection method used should be described in a step by step manner and accompanied by technical details. If there is not enough space on the table report, use appendixes.

Please document everything into a single PDF document.

- **Deliverable**

The required table report should have the following format.

Scenario 1			
Host	**Accessed or Compromised**	**How**	**Persistence**

Scenario 2			
Host	**Accessed or Compromised**	**How**	**Persistence**

Examples:

Scenario 1			
Host	**Accessed or Compromised**	**How**	**Persistence**
UATSERVER	YES	After obtaining administrator credentials the attacker compromised UATSERVER by remotely creating a malicious service… (mention how you detected that and also provide evidence)	YES (malicious scheduled task)
WIN10	YES	Eternal Blue exploit… (mention how you detected that and also provide evidence)	YES (malicious registry entry)

- **Recommended tools**

You are free to use any of the below tools

- Splunk
- ELK
- Wireshark (set up locally)
- Snort, Bro or Suricata (set up locally)
- Please note that you will need the OpenVPN client in order to connect to the exam environment

- **Hints for the best outcome**

- Keep track of all of your actions, searches, findings, etc. while you perform the Incident Response activities. (Mind mapping is your friend!)
- Dive into all the available functionality of the provided SIEM solutions

GOOD LUCK!