COS30015 IT Security

LAB 2 (week 2)

This lab seeks to provide you with the knowledge on how to plan a simple purple team exercise which involved both Red and Blue team personnel. It should expose you to some basic cyber tooling (attacker and defender, or offensive and defensive), MITRE TTPs, planning to identify and rectifying security vulnerabilities/breaches. All elements within this lab are planning only and should not actually be performed. The primary focus is identifying the following elements:

- The type of threat which will be sought to test
- Proposing a basic case study
- Proposing a simple testing scenario
- Creating a testing topology diagram
- Mapping out the steps involved
- Researching both attacker and defender, or offensive and defensive tools to fulfill the testing scenario
- Mapping high level MITRE TTPs

This lab document will guide you through the steps to complete the task. You can complete the task using the provided template.

Task 1: Threat Identification

Chose one threat area and research one of the provided examples. Seek to understand it's characteristics. For example:

- Brute force attacks: Seeks to try many different attempts to guide the correct authentication credentials. An attacker tries many times in succession, defenders can limit the number of tries to slow down or block an attacker.
- Enumeration: Seeks to gather information about a target. An attacker may gather system and user information which might assist with further objectives. Defenders can harden systems and log requests which might be of a suspicious nature to alert security staff.

Authentication

- Brute force attacks
- Password spray
- Credential stuffing

Reference: https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/, https://www.fortinet.com/resources/cyberglossary/brute-force-attack

Resource Hijacking

- Resource Exhaustion

Reference: https://en.wikipedia.org/wiki/Resource_exhaustion_attack

Malicious Software/Activity

- Enumeration

Resources: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/enumeration-ethical-hacking/

Sniffers

- Packet sniffing

Denial of Service

- Syn flood

Resource: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

While this list is not exhaustive, the examples provide simple testing scenarios.

Task 2: Basic case study

Having selected your chosen threat and example, research examples across industry relevant literature. Sources can include

- Government advisories
- Security vendors
- Media reporting
- Technology or cyber related articles

You want to address the following in your case study:

- Background of this threat
- Typical adversary trade craft
- Potential impact for an organisation

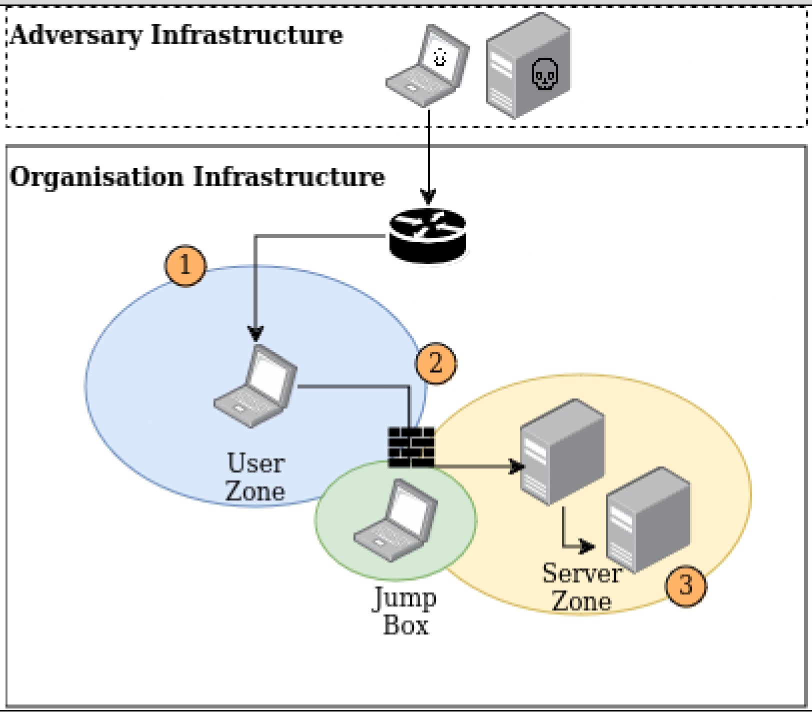
Some good resource can be found from:

- ACSC Advisories: https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories (choose Advisory for the type)
- CISA Advisories: https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A94

Task 3: Map out your testing scenario

Now having an idea about the threat and example you have researched, the next task it to create a basic testing scenario. This could be as simple as, *Use DoS tool against Web Server VM with out a firewall, record results, then apply the firewall with an appropriate rule to block the DoS attack and try again*, for example. Your aim it to begin to break it down into steps, and produce a topology.

An example of this may look like:

EXAMPLE
 Adversary Infrastructure Organisation Infrastructure 1 2 User Zone Jump Box Server Zone 3
Steps 1 Adversary notionally connect into the organisation’s environment 2 Adversary attempts to perform a DoS attack against the servers in step 3, performing a Syn flood 3 Servers are impacted depending on the enforcement of firewall rules

Map out a proposed scenario and produce a diagram listing the activities for each step. Free online tools such as “https://app.diagrams.net/” are helpful here.

Task 4: Tool/Activity Research

There are many resources on the Internet which document a range of tools and activities which can be used for both testing and defending against your chosen threat and example in your proposed testing scenario.

The next aim is to identify three tools or activities which can be used for the attacker side, and defender side. For example, identify three DoS tools, and then identify three tools which can be used to defend against a DoS attack. It’s best to stick with open source tools here, or those which come default in either Windows or Linux. Commercial tools are out of scope, and you should not recommend anything which requires Internet activity. A helpful hint here is look at tools often found in Kali Linux, and Defender tools which are either in a Linux environment or part of the native operating system (such as a firewall).

A note about Enumeration. This could be the use of a tool which enumerates open ports, or even a script which collects port information from running a series of commands. You’re welcome to be creative with this threat.

Identify your three tools or activities (again a possible enumeration script), and table the following information to help choose two tools or activities to use in your Purple team scenario. Use the following tables as a base structure.

Offensive Tools

Tool/Activity	Ease of Install	Amount of Documentation	Community Activity	Available Features to Produce Threat

Defensive Tools

Tool/Activity	Ease of Install	Amount of Documentation	Community Activity	Available Features Against Threat

Quick win references

- https://github.com/enaqx/awesome-pentest
- https://github.com/sbilly/awesome-security

Task 5: MITRE ATT&CK TTPs

Having identified your scenario and tools, you are required to document which TTPs the scenario activity will engage. Refer to the Enterprise ATT&CK matrix and at a high level:

- Identify which Tactics are relevant to your scenario
- Identify which Techniques are relevant to your scenario

These don’t need to be in-depth, but best to identify key ones which a related.