Purple Team Exercise Planning Template

Task 1

Threat	Example	Characteristic Identified
Denial of Service	DOS- SYN Flood Attack	• Availability of system resources, access or services is impacted • Can be achieved by a single or multiple hosts (distributed) • Different characteristics broadly exist for a Denial of Service attack, but it can consider either traffic flow or packet characteristics • Firewalls, intrusion prevention systems, web application firewalls, geo-blocking, load balancing are typical methods to counter

Task 2

Case summary of chose threat and example (max 4 paragraphs):

In 1996, Panix, one of the oldest internet service providers (ISPs), was the target of the first known distributed denial of service (DDoS) attack. The attack utilised a technique called a SYN Flood, which has since become a classic method in the DDoS attack arsenal. It targets the fundamental process of establishing a connection in the TCP/IP protocol suite. The attack exploits the way TCP (Transmission Control Protocol) manages the initiation of connections between a client and a server through a process known as the 'three-way handshake.'

In a SYN Flood attack, the attacker sends a large number of SYN packets to the target server, typically with spoofed (fake) source IP addresses. This flood of SYN packets causes the server to allocate resources for each incoming connection request, but because the source IP addresses are forged, the server never receives the final ACK packet. This leaves the connection 'half-open,' tying up the server's resources as it waits for a response that will never come. As the server's resources become increasingly consumed by these half-open connections, it eventually reaches a point where it can no longer process legitimate connection requests from other users. This results in a denial of service, where legitimate users are unable to access the services provided by the server.

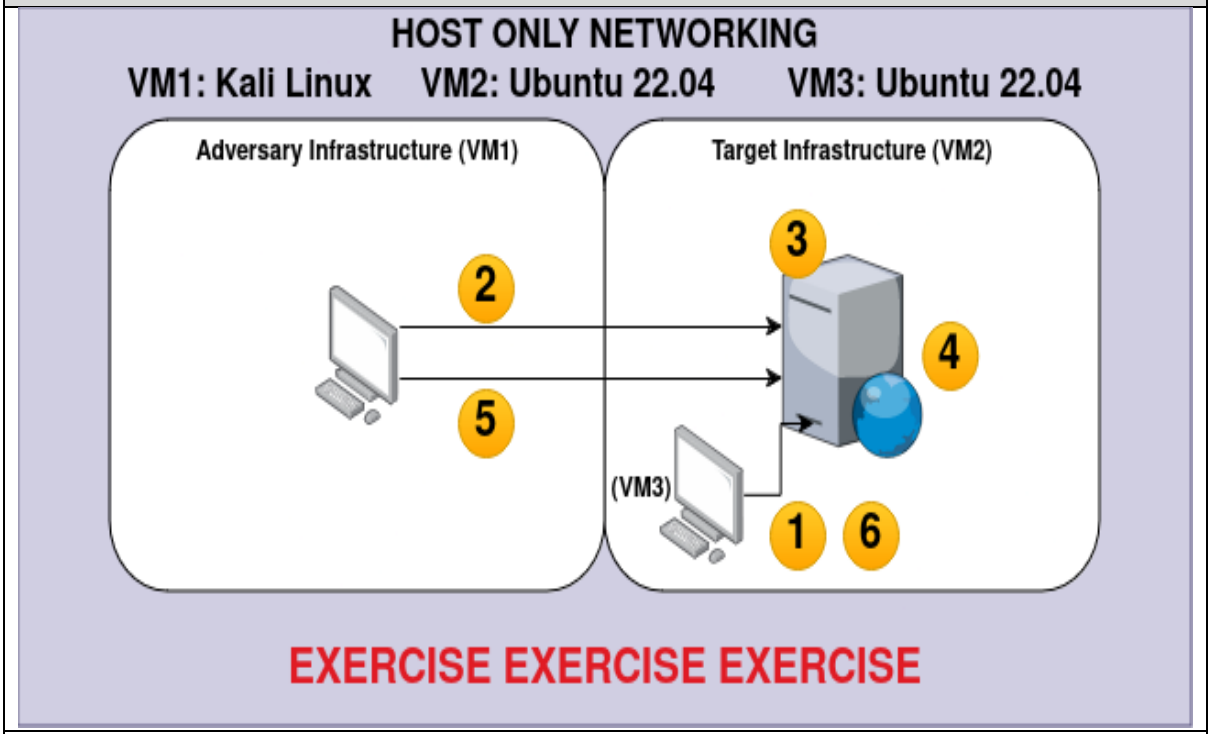
The SYN Flood attack caused Panix's internet services to go offline for several days. This outage was significant, particularly in the early days of the internet, where service disruptions could have severe consequences for users who relied on their connection for communication and business operations. As a service provider, Panix's credibility took a hit due to the extended downtime. Users who depended on Panix for reliable internet access were left frustrated, and the incident likely led to a loss of customer trust and potential business.

Government advisories, such as those from the Australian Cyber Security Centre (ACSC) and the Cybersecurity and Infrastructure Security Agency (CISA), provide essential guidance on mitigating resource exhaustion attacks. These advisories recommend robust traffic monitoring and filtering systems, setting resource usage limits, and using load balancing to distribute traffic evenly across

servers. By following these best practices, organisations can better prepare for and defend against the debilitating effects of resource exhaustion attacks.

Task 3

Outline your scenario with a diagram and steps



Pre-requisites

- Apache installed and available to the local network on the target device
- Host only connectivity between both VMs
- All tools used are either pre-installed with operating system or were installed prior, no Internet or other hosts/systems are being engaged

Steps

1. VM3 loads webpage from VM2, VM3 pings VM2
2. VM1 performs SYN Flood against VM2
3. VM2 crashes, pings continue to fail, and webpage reload unavailable on VM3
4. IPTables rule to mitigate SYN Flood applied on VM2
5. VM1 performs SYN Flood against VM2
6. VM3 successfully reloads html page and pings resume

Task 4

Record identified information

Offensive Tools

Tool/Activity	Ease of Install	Amount of Documentation	Community Activity	Available Features
hping3	• Simple installation • APT or YUM availability for Linux systems	• Well documented • Many user-based guides • Official documentation	• Active community • Open-source	• Customisable SYN packet crafting • High-rate packet sending
LOIC	• Cross-platform versions • Simple installation	• Well documented • Many user-based guides • Official documentation	• Semi-active community	• High traffic volume generation • Basic SYN Flood capability
Xerxes	• Requires compilation from source on some systems • Specific to certain Linux systems	• Includes some user guides and forums • Limited official documentation, mostly community-driven	• Security-focused forums	• Customisable attack vectors

Defensive Tools

Tool/Activity	Ease of Install	Amount of Documentation	Community Activity	Available Features
iptables	• Already installed by default in Linux	• Lots of documentation	• Lots of online resources given it's Linux native	• Custom rules to limit SYN requests • real-time blocking

SYN cookies	• Already installed by default in Linux	• Well documented, especially in Linux manuals • Kernel documentation and security guides	• Supported in most Linux communities	• Prevents SYN Flood by handling half-open connections efficiently
Snort	• Installation requires downloading and configuring	• Official guides and user-contributed tutorials	• Highly active community • Frequent updates and contributions	• Real-time detection of SYN Flood attacks

Task 5

Outline relevant MITRE TTPs:

Tactics

Impact (TA0040)

- **Objective**: The primary goal is to degrade or deny the availability of services, disrupting normal operations
- **SYN Flood Context**: By overwhelming the target server with a flood of SYN requests, the attacker exhausts the server's resources, leading to service unavailability

Techniques

Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)

- **Description**: Excessive amounts of SYN packets are sent, but the 3-way TCP handshake is never completed
- **SYN Flood Context**: Each OS has a maximum number of concurrent TCP connections that it will allow, this can quickly exhaust the ability of the system to receive new requests for TCP connections, thus preventing access to any TCP service provided by the server