Document Reference:	DoSRTU-1	Effective Date:	29 April 2024
Document Name:	Denial of Service Red Team Usecase	Expiry Date:	29 April 2025

Denial Of Service Red Team Usecase

Redback Operations

Document Owner:	Purple Team	Last Modified By:	Liya Thomas
Next Review Date:	17 June 2024	Last Modified on:	25 April 2024

KEEP
CALM
the
RED TEAM
IS HERE

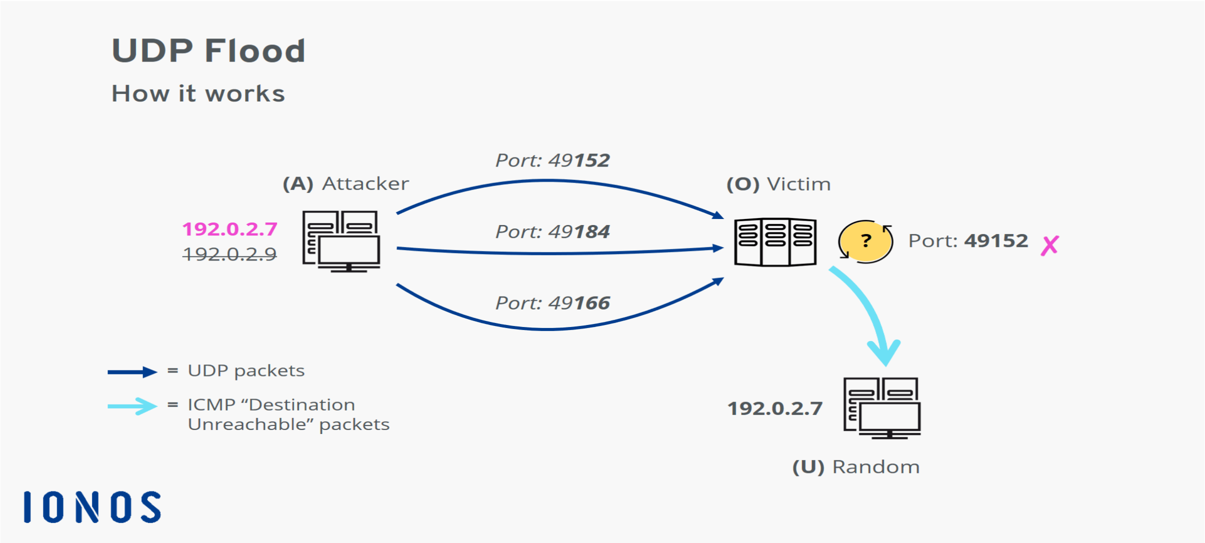
Version	Modified By	Approver	Date	Changes made
0.1	Liya Thomas		25 April 2024	First Draft
0.2	Joel Daniel		29 April 2024	Cosmetic changes
1.0	Liya Thomas	Joel Daniel	29 April 2024	Approved for publishing

Table of Contents

1 INTRODUCTION

In the digital realm, the specter of Denial of Service (DoS) incidents looms large, threatening the very fabric of organizations' network infrastructure and online operations. With nefarious actors wielding an arsenal of techniques, they can cripple target systems, leaving them inaccessible to rightful users. This playbook serves as a beacon for red teams, illuminating the intricate landscape of DoS attack types and furnishing them with the tools to fortify defenses against such pernicious threats.

2 UDP Flood



2.1 Objective:

The objective of conducting a UDP Flood attack is to overwhelm the target's network infrastructure by flooding it with UDP (User Datagram Protocol) packets, ultimately causing service disruption or downtime.

2.2 Red Team Usecases:

- Network Stress Testing: Determine the resilience of the target's network infrastructure by simulating a UDP Flood attack to assess its ability to handle such traffic spikes.

- Service Disruption: Disrupt the availability of critical services such as web servers, DNS servers, or online gaming platforms to cause financial loss or reputation damage to the target organization.

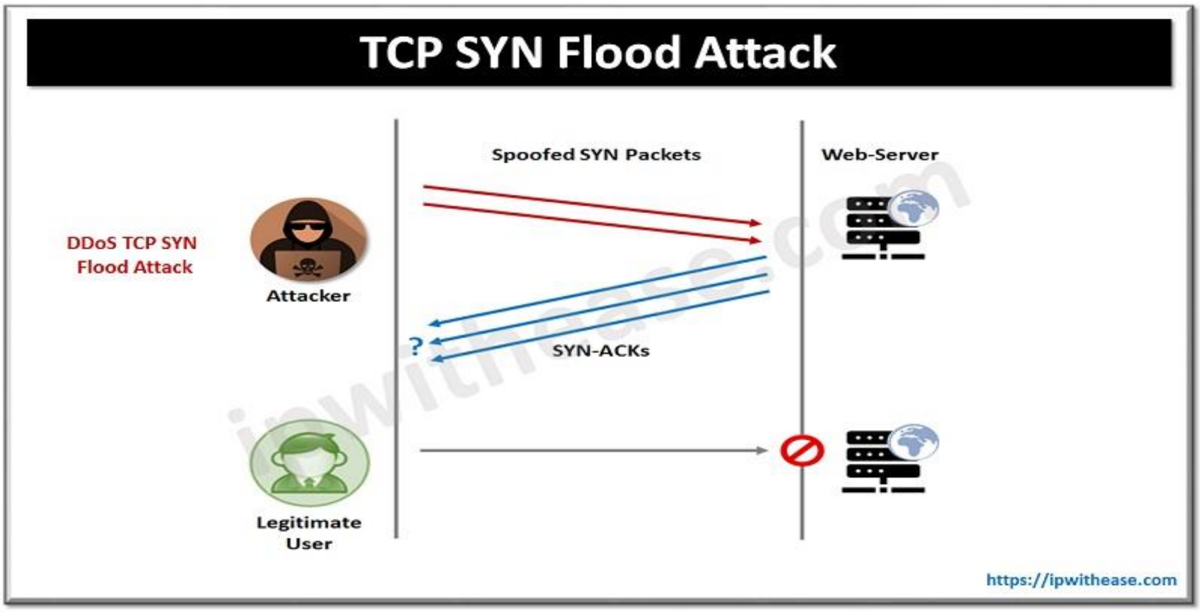
2.3 Steps:

1. Reconnaissance: Identify the target's network infrastructure, including IP addresses of servers and services to be targeted.
2. Tool Selection: Choose appropriate tools for conducting the UDP Flood attack, such as Hping3, UDP Unicorn, or LOIC (Low Orbit Ion Cannon).
3. Configuration: Configure the chosen tool to generate a high volume of UDP packets targeting the desired service or server. Specify the target IP address and port number.
4. Execution: Execute the attack by initiating the flood of UDP packets towards the target infrastructure.
5. Monitoring: Monitor the target's network for signs of service degradation or downtime caused by the flood of UDP packets.
6. Obfuscation (Optional): Employ techniques like IP spoofing or distributed botnets to obfuscate the source of the attack and evade detection or mitigation efforts.

2.4 Tools & Techniques:

- Hping3: Hping3 is a command-line tool used for generating and sending custom TCP/IP packets. It supports various protocols, including UDP, making it suitable for conducting UDP Flood attacks. Its flexibility allows users to customize packet size, frequency, and other parameters to suit the attack scenario.
- UDP Unicorn: UDP Unicorn is a lightweight tool specifically designed for UDP flooding. It enables attackers to generate a massive volume of UDP packets with minimal system resources. Its simple graphical interface makes it accessible even to less experienced attackers.
- LOIC (Low Orbit Ion Cannon): LOIC is an open-source network stress testing application. While originally intended for legitimate stress testing purposes, it has been repurposed by attackers for conducting DDoS attacks. LOIC's user-friendly interface and "Hive Mind" feature allow multiple users to coordinate simultaneous attacks, amplifying the impact of the UDP Flood.

3 TCP SYN Flood



3.1 Objective:

The objective of executing a TCP SYN Flood attack as a red team is to overwhelm a target server or network with a flood of TCP SYN packets, exhausting its resources and rendering it unavailable to legitimate users. This attack can serve as a means to test the resilience of network defenses, simulate real-world cyber threats, and uncover potential vulnerabilities in network infrastructure.

3.2 Steps:

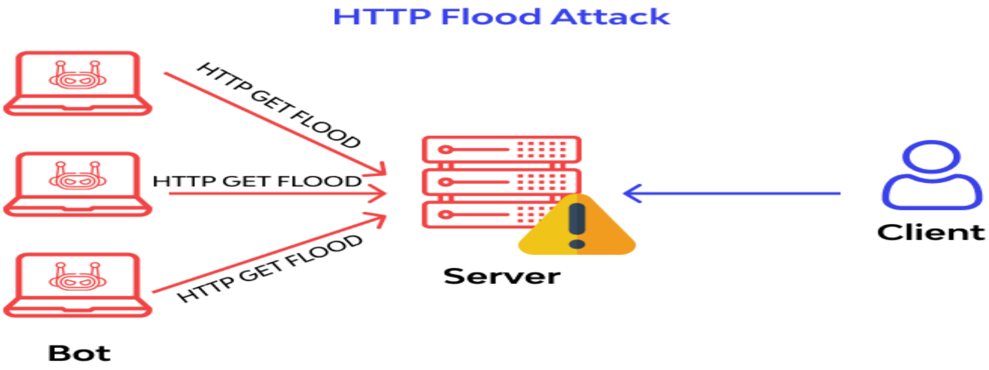
1. Reconnaissance: Identify the target network's IP address and determine the target server(s) to be flooded.
2. Tool Selection: Choose a suitable tool for conducting the TCP SYN Flood attack. Popular tools include Hping3, Scapy, and LOIC (Low Orbit Ion Cannon).
3. Configuration: Configure the chosen tool to generate a high volume of TCP SYN packets towards the target server(s).
4. Launch Attack: Initiate the TCP SYN Flood attack, sending a continuous stream of SYN packets to overwhelm the target server(s).
5. Monitoring: Continuously monitor the impact of the attack on the target network, observing for signs of network degradation or service disruption.

6. Adaptation: Adjust attack parameters if necessary to optimize effectiveness and evade detection by defensive measures.
7. Analysis: Analyze the results of the attack to identify weaknesses in network defenses and propose mitigation strategies.

3.3 Tools & Techniques:

- Hping3: Hping3 is a command-line tool used for generating TCP/IP packets. It offers flexibility in crafting packets and allows for the creation of customized TCP SYN Flood attacks. Its scripting capabilities enable automation and fine-tuning of attack parameters.
- Scapy: Scapy is a powerful interactive packet manipulation program written in Python. It provides a Python interface for crafting and sending packets, making it highly customizable for creating TCP SYN Flood attacks. Its versatility allows for the creation of complex packet sequences to evade intrusion detection systems.
- LOIC (Low Orbit Ion Cannon): LOIC is a network stress testing application designed for conducting Distributed Denial of Service (DDoS) attacks. It simplifies the process of launching TCP SYN Flood attacks by providing a user-friendly interface. However, it lacks the sophistication and customization options of more advanced tools like Hping3 and Scapy.

4 HTTP Flood



4.1 Objective:

The objective of the HTTP Flood DDoS playbook is to simulate a coordinated attack on a web server, overwhelming it with a high volume of HTTP requests.

4.2 Steps:

1. Reconnaissance:
   a. Gather information about the target web server, including its IP address, domain name, and any other relevant details.
   b. Identify potential vulnerabilities in the web server software or infrastructure that could be exploited during the attack.
2. Preparation:
   a. Set up the attack infrastructure, including the deployment of multiple attack machines or botnets capable of generating a large volume of HTTP requests.
   b. Configure the attack tools to target the specific URL or endpoints on the web server.
3. Execution:
   a. Initiate the HTTP Flood attack by sending a massive number of HTTP requests to the target web server simultaneously.
   b. Continuously monitor the performance of the attack to ensure that it is achieving the desired impact and overwhelming the target's resources.
4. Evasion:

   a. Implement evasion techniques to bypass any detection or mitigation measures deployed by the target organization, such as IP spoofing or distributed routing.
   b. Modify the characteristics of the attack traffic to mimic legitimate user behavior and avoid triggering alarms.

5. Persistence:
   a. Maintain the intensity of the attack over an extended period to maximize its impact on the target's operations.
   b. Dynamically adjust the parameters of the attack based on the target's response to evade detection and prolong the duration of the attack.

4.3 Tools & Techniques:

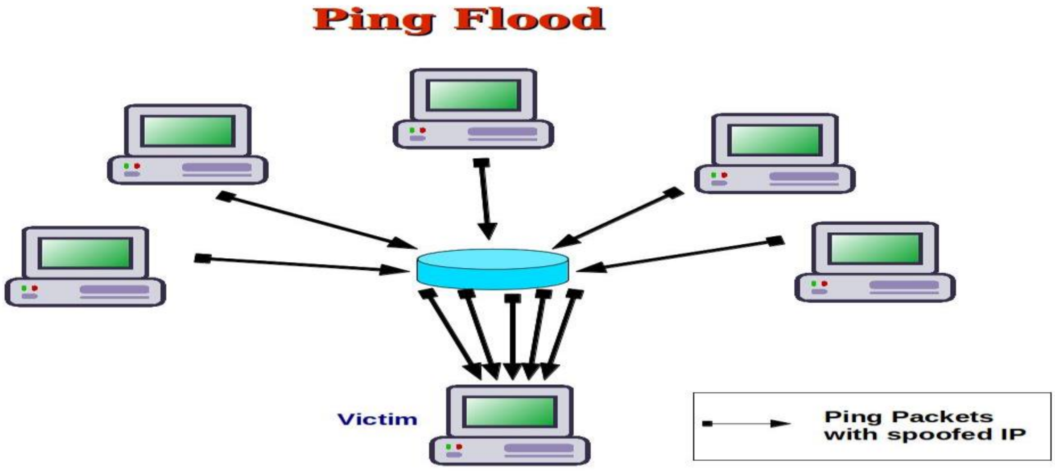
- HTTP Flood Tools:HULK (HTTP Unbearable Load King): A tool designed to generate a massive volume of HTTP requests, overwhelming the target web server's resources.
- LOIC (Low Orbit Ion Cannon): While originally developed for stress testing, it can be misused for DDoS attacks by flooding the target with HTTP requests.
- Xerxes: Another tool that enables users to launch HTTP Flood attacks, capable of generating a high volume of traffic to the target.
- Evasion Techniques:IP Spoofing: Falsifying the source IP address of the attack packets to make them appear to originate from legitimate sources, making it harder to trace back to the attacker.
- Randomized User Agents: Varying the User-Agent header in HTTP requests to mimic different types of web browsers and devices, making the attack traffic appear more like legitimate user activity.
- Session Persistence: Maintaining persistent connections to the target server to avoid detection by bypassing rate limiting or connection-based filtering mechanisms.

Monitoring Tools:

- Wireshark: A network protocol analyzer that can be used to capture and inspect the traffic generated by the HTTP Flood attack, allowing the attacker to analyze its effectiveness and detect any anomalies.
- Nmap: A versatile network scanning tool that can be used to identify open ports and services on the target web server, providing valuable information for reconnaissance and attack planning.

- Snort: An open-source intrusion detection system (IDS) that can be deployed to detect and alert on suspicious network activity, helping the attacker assess the effectiveness of evasion techniques and adjust the attack accordingly.

5 Ping Flood (ICMP Flood)



5.1 Objective:

The objective of executing a Ping Flood (ICMP Flood) attack as a red team is to overwhelm a target network or host with a flood of ICMP echo request packets, causing network congestion, service degradation, or denial of service. This attack helps assess the resilience of network infrastructure, test intrusion detection and prevention systems, and identify potential weaknesses in network defenses.

5.2 Steps:

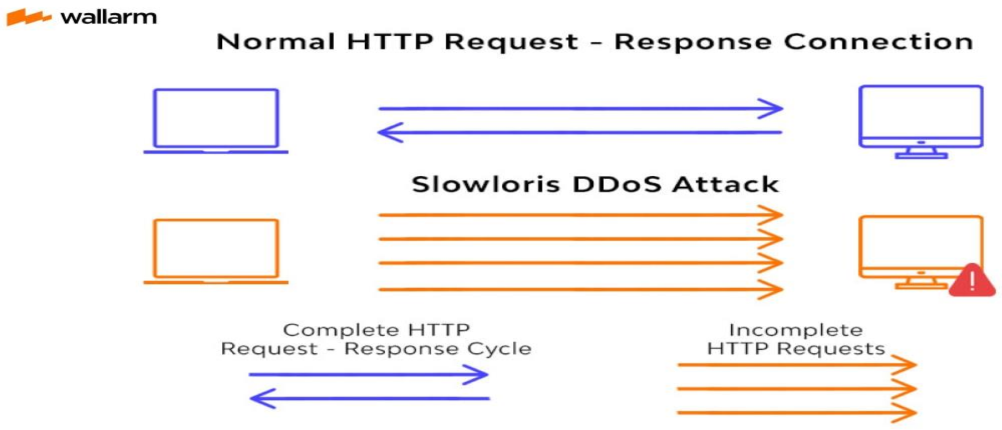
1. Reconnaissance: Identify the target network or host and determine the IP address(es) to be flooded.
2. Tool Selection: Choose a suitable tool for conducting the Ping Flood attack. Common tools include hping3, Scapy, and Nping.
3. Configuration: Configure the chosen tool to generate a high volume of ICMP echo request packets targeting the specified IP address(es).

4. Launch Attack: Initiate the Ping Flood attack, sending a continuous stream of ICMP echo request packets to overwhelm the target network or host.
5. Monitoring: Continuously monitor the impact of the attack on the target, observing for network latency, packet loss, and service disruptions.
6. Adaptation: Adjust attack parameters if necessary to optimize effectiveness and evade detection by network defenses.
7. Analysis: Analyze the results of the attack to identify vulnerabilities, assess the effectiveness of network defenses, and propose mitigation strategies.

5.3 Tools & Techniques:

- hping3: hping3 is a command-line tool used for sending custom TCP/IP packets. It supports various types of attacks, including Ping Flood, and allows for precise control over packet parameters such as TTL (Time To Live) and packet size. Its scripting capabilities enable automation and fine-tuning of attack parameters to suit specific objectives.
- Scapy: Scapy is a versatile packet manipulation tool written in Python. It provides a powerful interface for crafting and sending packets, making it ideal for conducting ICMP Flood attacks. Scapy's flexibility allows for the creation of custom packet payloads and the simulation of complex network scenarios.
- Nping: Nping is a command-line tool that is part of the Nmap suite of network scanning tools. It is designed for network packet generation, response analysis, and response time measurement. Nping's features include the ability to specify packet timing, payload data, and target hosts, making it suitable for conducting ICMP Flood attacks in a controlled manner.

6 Slowloris


wallarm
Normal HTTP Request - Response Connection
Slowloris DDoS Attack
Complete HTTP Request - Response Cycle
Incomplete HTTP Requests

6.1 Objective:

The objective of executing a Slowloris attack as a red team is to perform a low and slow HTTP Denial of Service (DoS) attack by keeping multiple connections to the target web server open for as long as possible, exhausting its resources and rendering it unavailable to legitimate users. This attack helps assess the resilience of web servers, test intrusion detection systems, and identify potential vulnerabilities in web application security.

6.2 Steps:

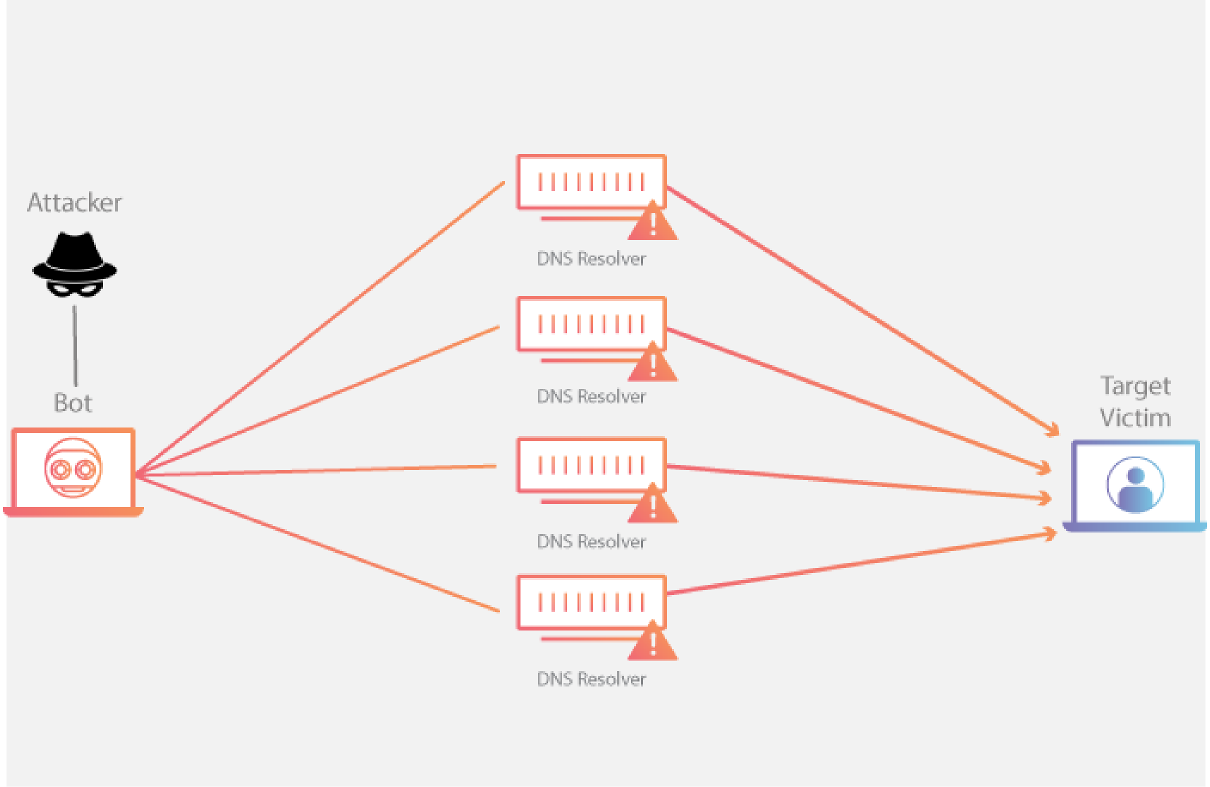
1. Reconnaissance: Identify the target web server and determine its IP address and listening ports.
2. Tool Selection: Choose a suitable tool for conducting the Slowloris attack. Common tools include Slowloris (Perl script), PyLoris (Python script), and R.U.D.Y (R-U-Dead-Yet).
3. Configuration: Configure the chosen tool to establish multiple concurrent connections to the target web server and send partial HTTP requests, keeping each connection open for an extended period.
4. Launch Attack: Initiate the Slowloris attack by sending HTTP headers slowly and incrementally to the target web server, consuming its available connections and resources.
5. Monitoring: Continuously monitor the impact of the attack on the target server, observing for increased response times, connection timeouts, and service disruptions.

6. Adaptation: Adjust attack parameters if necessary to prolong the duration of connections and evade detection by defensive measures.
7. Analysis: Analyze the results of the attack to identify weaknesses in web server configurations, assess the effectiveness of intrusion detection systems, and propose mitigation strategies.

6.3 Tools & Techniques:

- Slowloris (Perl script): Slowloris is a Perl script designed to perform a Slowloris-style HTTP DoS attack. It works by opening multiple connections to the target web server and sending partial HTTP requests, keeping each connection open by periodically sending additional headers. Slowloris's simplicity and effectiveness make it a popular choice for red teams conducting web server stress testing.
- PyLoris (Python script): PyLoris is a Python-based implementation of the Slowloris attack. It offers similar functionality to the original Slowloris script but is written in Python, making it more accessible to users familiar with the Python programming language. PyLoris provides additional features such as support for SSL/TLS connections and customizable attack parameters, enhancing its versatility for red team engagements.
- R.U.D.Y (R-U-Dead-Yet): R.U.D.Y is another HTTP DoS attack tool that follows a similar slow and low approach to Slowloris. It focuses on sending POST requests with a large content length, keeping each connection open by sending a continuous stream of POST data slowly. R.U.D.Y's ability to target web applications vulnerable to resource exhaustion makes it a valuable tool for red teams assessing web server security.

7 DNS Amplification



7.1 Objective:

The objective of executing a DNS Amplification attack as a red team is to leverage vulnerable DNS servers to amplify a small number of DNS queries into a flood of responses directed towards a target victim, causing network congestion, service disruption, or denial of service. This attack helps assess the resilience of network infrastructure, test the effectiveness of DDoS mitigation measures, and identify potential vulnerabilities in DNS server configurations.

7.2 Steps:

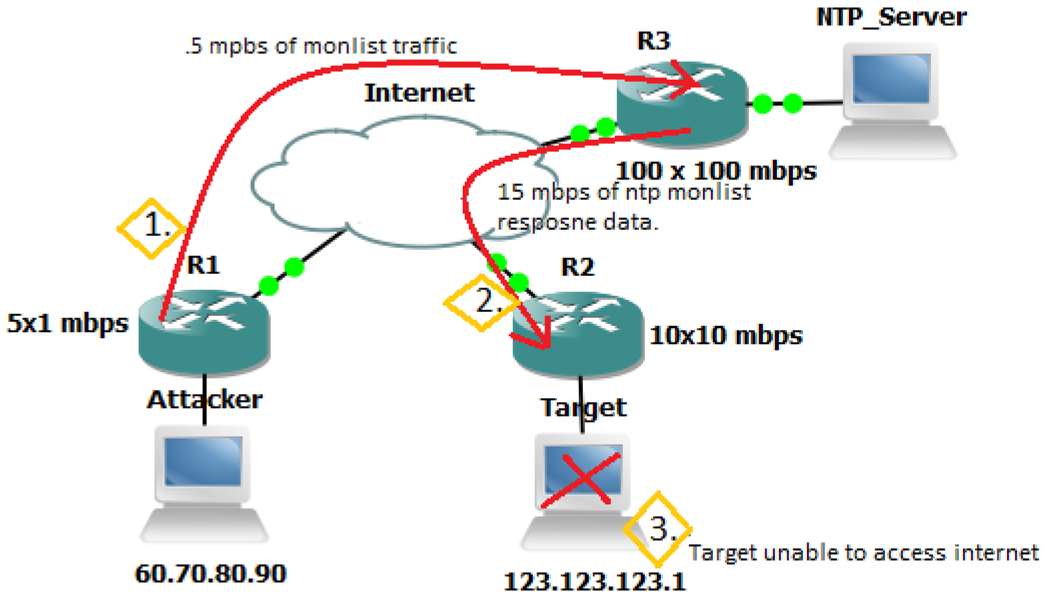
1. Reconnaissance: Identify vulnerable DNS servers that support DNS amplification, typically open or misconfigured DNS resolvers with recursion enabled.
2. Tool Selection: Choose a suitable tool for conducting the DNS Amplification attack. Common tools include DNSRecon, dnsenum, and dnsmap for reconnaissance, and tools like DNSChanger, dns2tcp, and Nslookup for performing the actual attack.
3. Configuration: Configure the chosen tool to send DNS queries with a spoofed source IP address of the target victim and a DNS query for a large DNS record type (e.g., DNS ANY query).
4. Launch Attack: Initiate the DNS Amplification attack by sending crafted DNS queries to the vulnerable DNS servers, causing them to send large responses to the target victim's IP address.
5. Monitoring: Continuously monitor the impact of the attack on the target victim, observing for increased network traffic, DNS response times, and service disruptions.
6. Adaptation: Adjust attack parameters if necessary to optimize amplification and evasion of detection by network defenses or DNS monitoring systems.
7. Analysis: Analyze the results of the attack to identify weaknesses in DNS server configurations, assess the effectiveness of DDoS mitigation measures, and propose mitigation strategies.

7.3 Tools & Techniques:

- DNSRecon: DNSRecon is a DNS enumeration tool designed for reconnaissance purposes. It helps identify DNS servers, zone transfers, and DNS records associated with a target domain. DNSRecon's features include brute-force DNS subdomain enumeration and reverse DNS lookups, making it useful for identifying potential targets for DNS Amplification attacks.
- DNSChanger: DNSChanger is a tool used for crafting and sending DNS queries with custom parameters. It supports various DNS record types and allows for the spoofing of source IP addresses, making it suitable for performing DNS Amplification attacks. DNSChanger's simplicity and effectiveness make it a preferred choice for red teams conducting network stress testing.
- Nslookup: Nslookup is a command-line tool used for querying DNS servers to obtain DNS information. While not specifically designed for conducting DNS Amplification attacks, Nslookup can be used to send DNS queries to vulnerable DNS servers for

reconnaissance purposes. Its simplicity and availability on most operating systems make it a handy tool for red teams during penetration testing engagements.

8 NTP Amplification



8.1 Objective:

The objective of executing an NTP (Network Time Protocol) Amplification attack as a red team is to exploit vulnerable NTP servers to amplify a small number of NTP queries into a flood of responses directed towards a target victim, causing network congestion, service disruption, or denial of service. This attack helps assess the resilience of network infrastructure, test the effectiveness of DDoS mitigation measures, and identify potential vulnerabilities in NTP server configurations.

8.2 Steps:

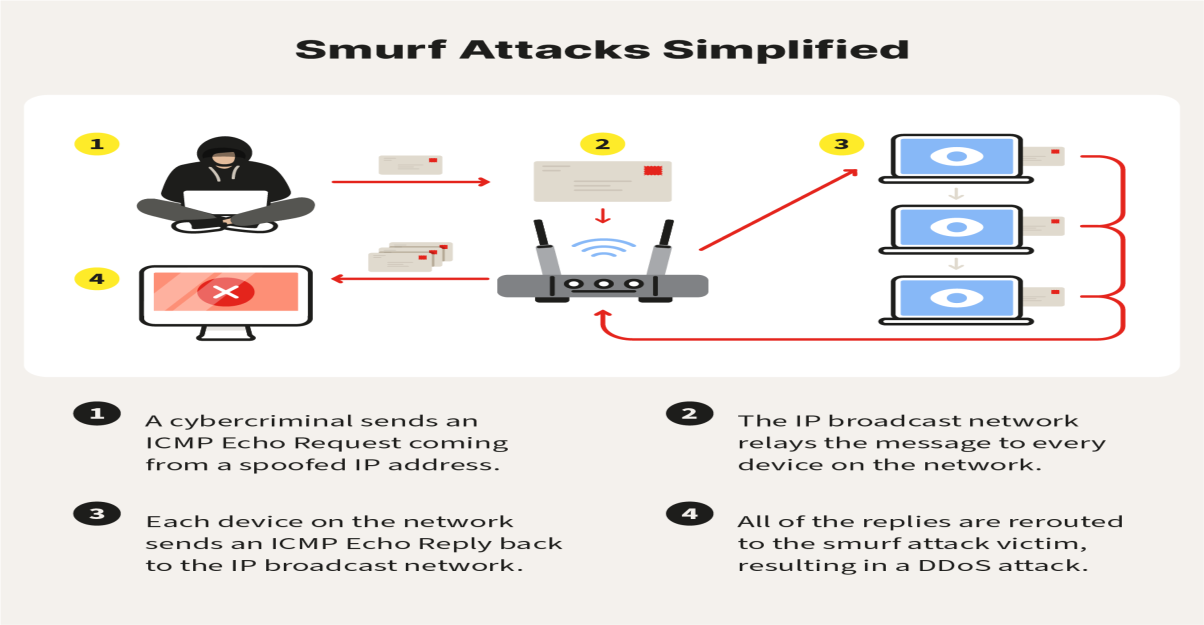
1. Reconnaissance: Identify vulnerable NTP servers that support NTP amplification, typically open or misconfigured NTP servers with monlist enabled.
2. Tool Selection: Choose a suitable tool for conducting the NTP Amplification attack. Common tools include Nmap, NTPScan, and NTPMonlist for reconnaissance, and tools like NTPDOS, NTPFlood, and NTPReflection for performing the actual attack.
3. Configuration: Configure the chosen tool to send NTP queries with a spoofed source IP address of the target victim and request the monlist command, which triggers the NTP server to send a list of the last clients that have connected to it.
4. Launch Attack: Initiate the NTP Amplification attack by sending crafted NTP queries to the vulnerable NTP servers, causing them to send large responses to the target victim's IP address.
5. Monitoring: Continuously monitor the impact of the attack on the target victim, observing for increased network traffic, NTP response times, and service disruptions.
6. Adaptation: Adjust attack parameters if necessary to optimize amplification and evasion of detection by network defenses or NTP monitoring systems.
7. Analysis: Analyze the results of the attack to identify weaknesses in NTP server configurations, assess the effectiveness of DDoS mitigation measures, and propose mitigation strategies.

8.3 Tools & Techniques:

- Nmap: Nmap is a versatile network scanning tool that can be used for reconnaissance purposes. It includes scripts like "ntp-monlist" to identify NTP servers vulnerable to amplification attacks by querying for the monlist command. Nmap's extensive feature set and scriptable nature make it a valuable tool for red teams conducting vulnerability assessments.
- NTPDOS: NTPDOS is a tool specifically designed for launching NTP amplification attacks. It allows users to specify target NTP servers, spoofed source IP addresses, and other parameters to conduct large-scale NTP amplification attacks. NTPDOS's simplicity and effectiveness make it a preferred choice for red teams assessing network security.
- NTPReflection: NTPReflection is another tool used for NTP amplification attacks. It automates the process of sending crafted NTP queries to vulnerable NTP servers and analyzing the responses to measure the amplification factor. NTPReflection's user-

friendly interface and comprehensive reporting capabilities make it suitable for red teams conducting penetration testing engagements.

9 Smurf Attack



Smurf Attacks Simplified

1 A cybercriminal sends an ICMP Echo Request coming from a spoofed IP address.

2 The IP broadcast network relays the message to every device on the network.

3 Each device on the network sends an ICMP Echo Reply back to the IP broadcast network.

4 All of the replies are rerouted to the smurf attack victim, resulting in a DDoS attack.

9.1 Objective:

The objective of executing a Smurf Attack as a red team is to flood a target network with a large volume of ICMP echo request packets, directing them to the broadcast address of the network, causing network congestion, service disruption, or denial of service. This attack helps assess the resilience of network infrastructure, test the effectiveness of DDoS mitigation measures, and identify potential vulnerabilities in network configurations.

9.2 Steps:

1. Reconnaissance: Identify the target network and determine its broadcast address.
2. Tool Selection: Choose a suitable tool for conducting the Smurf Attack. Common tools include Smurf, fragrouter, and hping3.
3. Configuration: Configure the chosen tool to send ICMP echo request packets with a spoofed source IP address of the target victim to the broadcast address of the target network.

4. Launch Attack: Initiate the Smurf Attack by sending a flood of ICMP echo request packets to the broadcast address, causing all hosts within the network to reply to the spoofed source IP address, overwhelming the target victim.
5. Monitoring: Continuously monitor the impact of the attack on the target victim, observing for increased network traffic, ICMP response times, and service disruptions.
6. Adaptation: Adjust attack parameters if necessary to optimize effectiveness and evade detection by network defenses or intrusion detection systems.
7. Analysis: Analyze the results of the attack to identify weaknesses in network configurations, assess the effectiveness of DDoS mitigation measures, and propose mitigation strategies.

9.3 Tools & Techniques:

- Smurf: Smurf is a tool specifically designed for conducting Smurf Attacks. It allows users to specify the target victim's IP address and the broadcast address of the target network, as well as the number of ICMP echo request packets to send. Smurf's straightforward interface and ease of use make it a preferred choice for red teams assessing network security.
- fragrouter: fragrouter is a tool used for conducting various network attacks, including Smurf Attacks. It enables the fragmentation and routing of packets to evade detection by intrusion detection systems and firewalls. fragrouter's advanced features, such as packet fragmentation and manipulation, enhance its effectiveness for red teams during penetration testing engagements.
- hping3: hping3 is a versatile command-line tool for sending custom TCP/IP packets. While not specifically designed for Smurf Attacks, it can be used to craft and send ICMP echo request packets with a spoofed source IP address. hping3's flexibility and scripting capabilities make it suitable for conducting a wide range of network attacks, including Smurf Attacks.

10 Conclusion

In closing, this playbook acts as a guardian for red teams, imparting profound insights into an array of Denial of Service attack types. From the relentless barrage of UDP Floods to the cunning exploitation of DNS Amplification, each attack method is dissected, analyzed, and met with formidable countermeasures. By embracing this knowledge, red teams can navigate the turbulent waters of cyber warfare, fortify organizational defenses, and preserve the sanctity of critical assets and services from the tumult of disruptive cyber threats.

References

UDP Flood - https://www.ionos.com/digitalguide/fileadmin/DigitalGuide/Schaubilder/how-the-udp-flood-works.png

TCP SYN Flood- https://i1.wp.com/ipwithease.com/wp-content/uploads/2022/12/TCP-SYN-FLOOD-ATTACK.jpg?fit=800%2C455&ssl=1&is-pending-load=1

HTTP Flood- https://www.radware.com/RadwareSite/MediaLibraries/Images/DDoS-Application-Attack-Hub/what-is-http-flood.jpg

Ping Flood (ICMP Flood)- https://3.bp.blogspot.com/-im7yvv9U3iY/VuBCgcdLBxI/AAAAAAAAAZw/GGlc-ke9l_8/s1600/PingFlood.jpg

Slowloris- https://assets.website-files.com/5ff66329429d880392f6cba2/62750dd2d15f280e6cc03651_Slowloris.jpg

DNS Amplification- https://cfassets.www.cloudflare.com/slt3lc6tev37/2JmKP07Mi6jYbACILN84VI/9a91d91ecc1f414aa89ae001dbfce393/Learning_Center_DDoS_Diagrams_clean.png

NTP Amplification- https://www.datayard.us/wpcontent/uploads/2015/02/ntp_ddos_1.png

Smurf attack- https://us.norton.com/content/dam/blogs/images/norton/am/smurf-attacks-simplified.png