Denial-of-Service attack

Presenter: Nikee, Ragavi and Xi (Lucas)

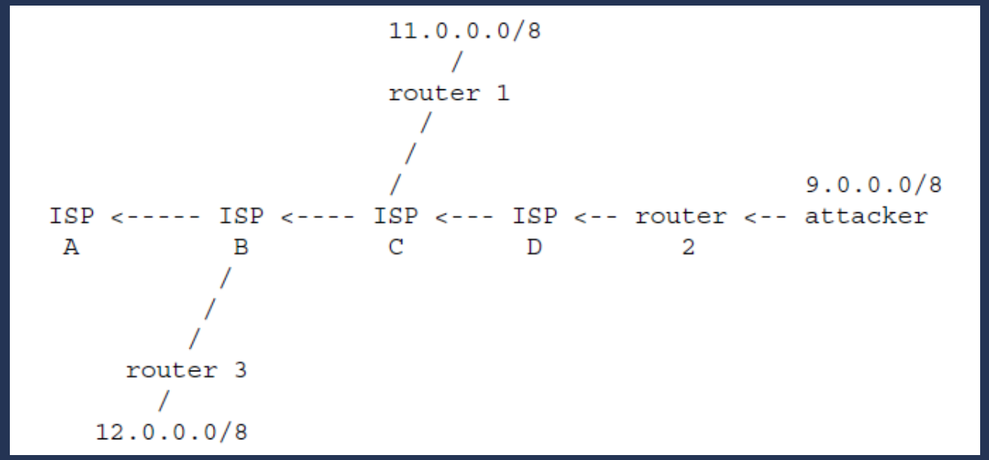
Introduction

- A cyber attack where the machine or network resource is made unavailable for use by temporarily or indefinitely disrupting services of the host connected to the Internet.
- In Denial of Service(DoS), the attacker floods the target system with a chain of superfluous requests to overload the system so as to avert the legitimate requests from being executed
- Also known as the Transmission Control Protocol (TCP) SYN attack, the SYN Flood attack is one of the major flooding technique used for performing the DoS attack.
- SYN flood attack is based on exploiting the standard TCP three-way handshake. In this, a large number of SYN's are sent without sending the corresponding acknowledgments. As a result, the server is left waiting for the non-existent acknowledgments.

Network Ingress Filtering

- Consider a TCP SYN attack launched using a source address, the target host attempts to reserve resources waiting for a response.
- The attacker then repeatedly changes the bogus source address on each new packet sent, thus exhausting additional host resources.
- Network Ingress filtering is used for defeating the Denial of Service attacks that employ IP source address spoofing.
- Using this technique, it will prohibit an attacker from launching an attack of using forged source addresses that do not conform to ingress filtering rules.

Consider the following scenario



- In this, the attacker resides within 9.0.0.0/8, which is provided Internet connectivity by an ISP.
- An input traffic filter on the ingress (input) link of "router 2", which provides connectivity to the attacker's network, restricts traffic to allow only traffic originating from source addresses within the 9.0.0.0/8 prefix.
- Hence, it prohibits an attacker from using "invalid" source addresses which reside outside of this prefix range.

Distributed

denial-of-service attack

- In a Distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the target system originates from many different sources.
- This makes it impossible to terminate the attack by just blocking a sole source.
- As a consequence, it is impossible to stop the attack simply by using ingress filtering.
- It also makes it very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.
- As an augmentation to DDoS, many attacks additionally involve forging of IP sender addresses, so that the location of the attacking machines cannot easily be identified and defeated.

DDOS Attack Tools

- Low Orbit Ion Cannon (LOIC): It is flooding tool that produces excessive volumes of TCP, UDP, or HTTP traffic to subject server to a heavy network load.
- High Orbit Ion Cannon (HOIC): It is a cross platform script for sending HTTP POST and GET requests was wrapped in an easy to use GUI. It used to target the U.S Department of Justice.
- Hping: It is a command line utility used to send large volumes of TCP traffic to a target while spoofing the source IP addresses.
- Slowloris : It uses a very slow HTTP requests by sending HTTP headers to the target site in tiny chunks as slowly as possible which makes the server to wait for the headers to arrive and thus creating DOS.
- R.U.D.Y: RUDY achieves DOS by using long form field HTTP POST submission. It causes the application to await the nonstop posts in order to do processing.
- Botnets: Botnets are large collection of compromised computers, often called ―zombies‖, infected with malware that allows an attacker to control them.

Demo Session

Programming is fun

Application is playable

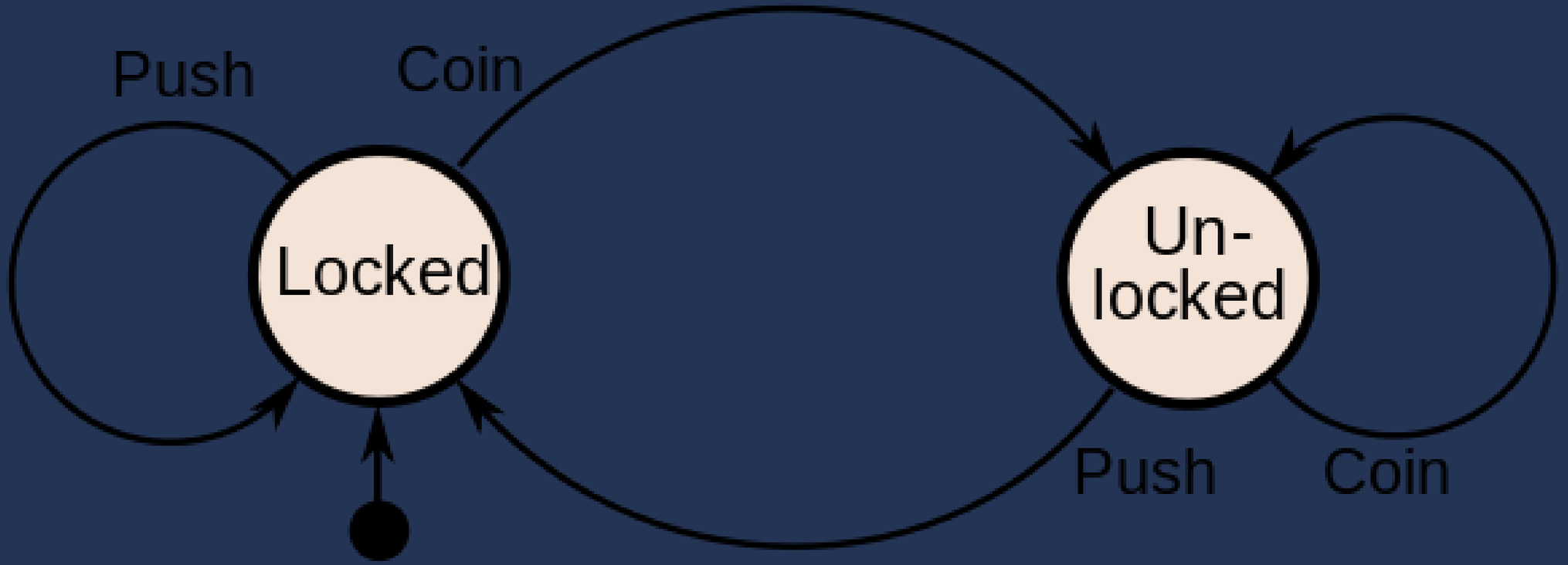
Data visualization is intuitive

RegEx-DoS

- Introduction: is an algorithmic complexity attack that produces a denial-of-service by providing a regular expression that takes a very long time to evaluate.
- Fact: The attack exploits the fact that most regular expression implementations have exponential time worst case complexity: the time taken can grow exponentially in relation to input size.
- Result: An attacker can thus cause a program to spend an unbounded amount of time processing by providing such a regular expression, either slowing down or becoming unresponsive.

More about Regular Expression

Regular expression matching can be done by building a finite-state automaton.


Push
Coin
Locked
Un-
locked
Push
Coin

the engine may convert it to a deterministic finite-state automaton (DFA) and run the input through the result;

the engine may try one by one all the possible paths until a match is found or all the paths are tried and fail ("backtracking").

Let's see how much time some RegEx take to evaluate

Detection Of DoS

- All detection methods define an attack as an abnormal and noticeable deviation of some statistic of the monitored network traffic workload.
- Each of the attack detection techniques include an evaluation of a different statistic of network traffic.

Activity Profiling

- Monitoring a network packet's header information offers an activity profile.
- The activity profile is the average packet rate for a network flow, which consists of consecutive packets with similar packet fields (such as address, port,and protocol).
- The elapsed time between consecutive matching packets determines the flow's average packet rate or activity level.
- The total network activity can be measured as the average packet rates of all inbound and outbound flows.
- To avoid high-dimensionality issues, individual flows with similar characteristics can be clustered.
- Each cluster's activity level is the summation of constituent flows.

An attack is indicated by either of the following

- Increasing activity levels among clusters, which can indicate a few attacking agents increasing their attack-generation rate.
- An increase in the overall number of distinct clusters, which can represent many distributed attacking agents (as in a DDoS).

Wavelet Analysis

- Wavelet analysis describes an input signal in terms of spectral components.
- Wavelets provide for concurrent time and frequency description, and can thus determine the time at which certain frequency components are present.
- For detection applications, wavelets separate out anomalous signals from background noise; the input signal contains both.
- Ideally, the signal and noise components will dominate in separate spectral windows.
- Analyzing each spectral window's energy determines the presence of anomalies.

Prevention of DoS

Prevention tries to stop the event from happening in the first place whereas mitigation tries to limit the damage

Examples of Denial of Service attacks launched against web applications include:

1. Attempts to "flood" web applications, thereby preventing legitimate user traffic
2. Attempts to disrupt service to a specific system or person, e.g., blocking user access by repeated invalid login attempts resulting in the account's suspension
3. Jamming the application-database connection by crafting CPU-intensive SQL queries

Preventing Denial of Service Attacks

With dotDefender web application firewall you can avoid DoS attacks because dotDefender inspects your HTTP traffic and checks their packets against rules such as to allow or deny protocols, ports, or IP addresses to stop web applications from being exploited.

- Easy installation on Apache and IIS servers
- Strong security against known and emerging hacking attacks
- Requires no additional hardware, and easily scales with your business

Preventing DoS attacks may not always be possible, but with a strong defense, enterprises can reduce their impact and recover quickly.

Minimize the attack surface

- This provides tremendous benefits for preventing DoS attacks because attacker's hits on unneeded systems are completely avoidable.
- A firewall rule base analysis can provide great insight into what's needed and what can go.

Find and fix

- Find and fix the known vulnerabilities that can facilitate denial-of-service attacks. Many internet-accessible systems and applications are under-protected.
- Such flaws usually come in the form of missing firmware and software updates on perimeter systems as well as on server operating systems. Again, this is completely preventable.

Use a next-generation firewall or a DoS protection appliance.

- A near-ideal solution is to use a cloud-based DoS protection service. Many enterprises rely on such vendors to offload DoS traffic when the going gets rough. Just be sure to vet these companies and choose a solution in advance.

Know what's normal on your network.

- Most people either don't have that level of visibility or they simply cannot keep up due to the number of systems and the volume of network traffic.
- Ingress filtering, for example, is a valuable technique for preventing DoS attacks.

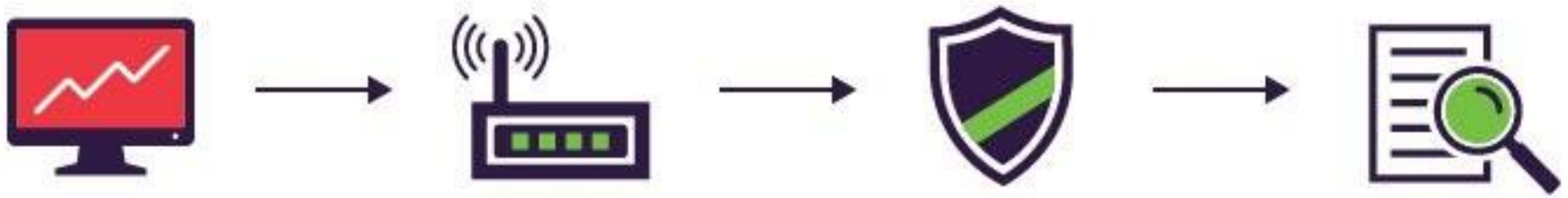
Make a plan

- Lack of formal, documented incident response plans. A well-written incident response plan will address denial-of-service and attacks provide general guidance on who needs to be called, specific steps that need to be taken to minimize the impact of such an attack and how to clean up and move forward afterwards.

Mitigation of DoS

1. Detection – The identification of traffic flow deviations that may signal the buildup of a DDoS assault. Effectiveness is measured by your ability to recognize an attack as early as possible, with instantaneous detection being the ultimate goal.
2. Diversion – Traffic is rerouted away from its target, either to be filtered or completely discarded.
3. Filtering – DDoS traffic is weeded out, usually by identifying patterns that instantly distinguish between legitimate traffic (i.e., humans, API calls and search engine bots) and malicious visitors. Responsiveness is a function of your being able to block an attack without interfering with your users' experience. The aim is for your solution to be completely transparent to site visitors.
4. Analysis – Security logs are reviewed to gather information about the attack, both to identify the offender(s) and to improve future resilience. The process's effectiveness relies on the existence of detailed security logs that can offer granular visibility into the attack traffic.

DDoS Mitigation Stages



Detection

Abnormal traffic flows are identified

Diversion

Traffic is redirected (BGP/DNS routing)

Filtering

DDoS traffic is weeded out while clean traffic is passed on

Analysis

Security logs are used to improve resilience

Thank you, Q&A