

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Presentators: **Komal, Andrew, Lax, Mini, and Santiago**



Table of Contents

This document contains the following resources:



Network Topology & Critical Vulnerabilities



Alerts Implemented



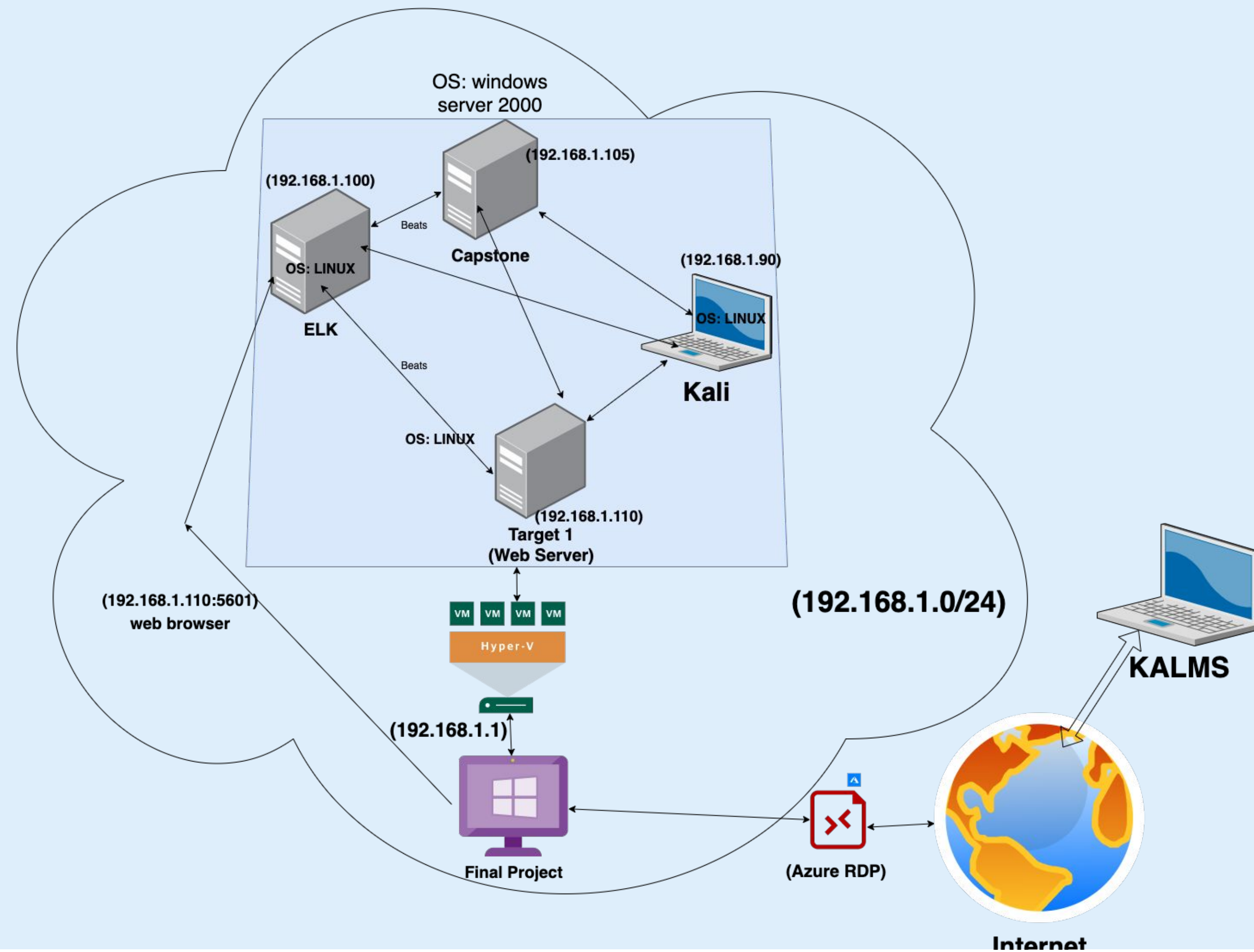
Hardening



Implementing Patches

Network Topology & Critical Vulnerabilities

Network Topology



Network

Address

Range:192.168.1.0/24

Netmask:255.255.255.0

Gateway:192.168.1.1

Machines

IPv4:192.168.1.100

OS: Linux

Hostname: ELK

IPv4:192.168.1.110

OS: Linux

Hostname: Target 1

IPv4:192.168.1.105

OS: Windows

Hostname: Capstone

IPv4:192.168.1.90

OS: Kali Linux

Hostname: Kali

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
CWE-400	DDOS	Crash, Exit, or Restart; DoS: Resource Consumption (CPU); DoS: Resource Consumption (Memory); DoS: Resource Consumption (Other)
CWE-307	Brute force attack	An attacker could perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account.
CWE-89	SQL Injection	Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL injection vulnerabilities.
CWE - 22	File Inclusion Exploits	File inclusion exploits happen when vulnerable PHP code is used to load remote files that are in the server. File inclusion exploits are one of the most common ways an attacker can gain access to wp-config.php which is in fact the WordPress configuration file.











The background of the slide is a dark gray field filled with a complex, repeating pattern of geometric shapes. These shapes include squares and triangles of various sizes, some of which are slightly offset or layered, creating a three-dimensional, crystalline effect. The overall tone is monochromatic and modern.

Alerts Implemented

Excessive HTTP Errors

Queries packetbeat indices for http status code responses

- **Metric :** Packetbeat
- **What is the threshold it fires at?** Triggers when the grouped count over top 5 https status response code exceeds 400 in the last 5 minutes

<input type="checkbox"/> ID	Name	State	Last fired	Last triggered	Comment	Actions
<input type="checkbox"/> 9b24fb3b-ac40-454d-8c98-0430c72603f4	HTTP request size monitor	✓ OK		a few seconds ago		 
<input type="checkbox"/> 897a4718-b3e2-4c7b-9413-42b565a82da0	Excessive HTTP Errors	✓ OK		a few seconds ago		 
<input type="checkbox"/> a9914096-329e-4f62-8038-944f4d0dd599	HTTP request	✓ OK		a few seconds ago		 
<input type="checkbox"/> de29a9d8-0413-449f-ada4-1c4e11b3cb0f	CPU usage monitor	✓ OK	4 hours ago	a few seconds ago		 
<input type="checkbox"/> f5235a10-0d06-43f2-b9ea-81a594c84840	Port Scan	✓ OK		a few seconds ago		 

HTTP Request Size

- **Metric:** Packetbeat-7.7.0-2021.03.19-000001
- **Threshold:** Total Http requests bytes is above 3500 for last minute.

Name

HTTP Request Size Monitor

Indices to query

packetbeat-7.7.0-2021.03.19-000001 ×

Time field

@timestamp

Run watch every

1



minute

Use * to broaden your query.

Match the following condition

WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute

and when fired:

<input type="checkbox"/>	fb758d3d-00f9-4861-b385-c4eb3701e168	HTTP Request Size Monitor	✓ OK	a few seconds ago		
--------------------------	--------------------------------------	---------------------------	------	-------------------	---	---

CPU Usage Monitor

- **Metric:** Metricbeat
- **Threshold:** When max() of system.process.cpu.total.pct over all documents is above 0.5 for the last 5 minutes

Name

CPU Usage Monitor

Indices to query

metricbeat-* ×

Time field

@timestamp

Run watch every



1

minute

Use * to broaden your query.

Match the following condition

WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

<input type="checkbox"/>	<div>c98b479f-31c2-4942-ad1f-5aafd83a06d5</div>	CPU Usage Monitor	✓ OK	9 hours ago	a minute ago		
--------------------------	---	-------------------	------	-------------	--------------	---	---

Hardening Against Brute-Force Attack on Target 1

Patch: Ensure passwords are complex, use two factor authentication, and make the root user inaccessible via SSH

Why It Works: Complex passwords are harder to guess and take much longer to guess. Using two factor authentication makes it much harder for malicious parties to get access to the clients server and finally, hackers that can log in to the server through roots account via SSH can cause damage and so it saves trouble to disallow root access via SSH

How to install it :

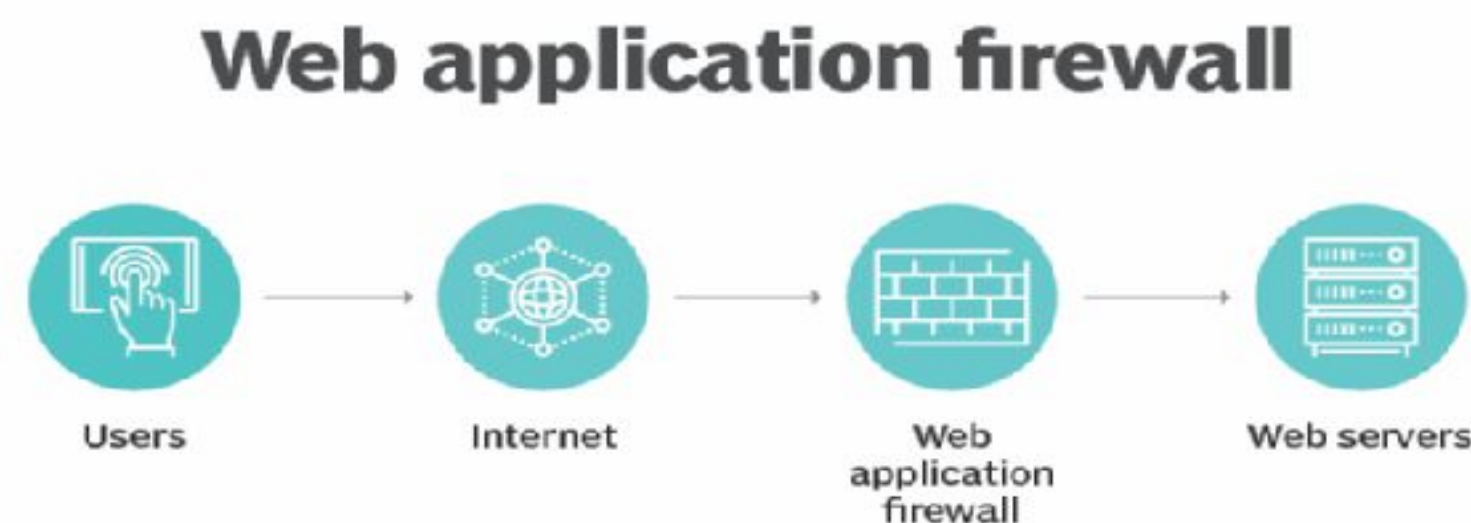
```
nano /etc/ssh/sshd_config
```

```
(change) #PermitRootLogin yes (to) PermitRootLogin no
```

```
/etc/init.d/sshd restart
```

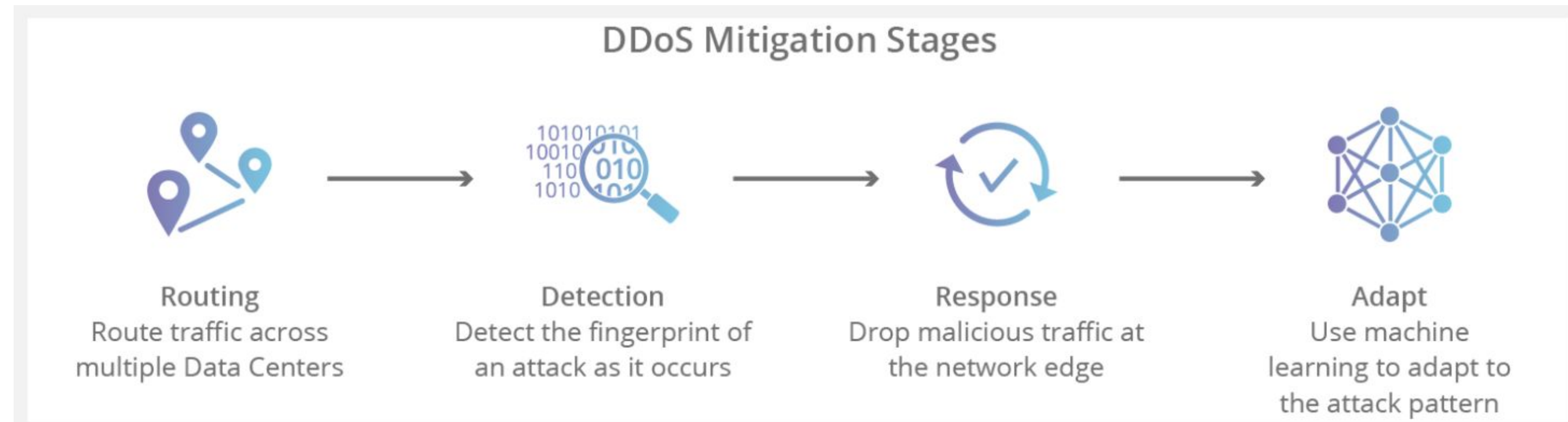
```
systemctl restart sshd
```

```
service sshd restart
```



Hardening Against Spike in HTTP Request Size (DDOS) on Target 1

- **Vulnerability:** DDOS Attack
- **Patch:** There are no reliable patches or software updates that have been proven to control DDOS attacks but there are DDoS mitigation services, e.g cloudflare.
- **Why It Works:** DDOS mitigation services, detect suspected DDOS attacks, reroute them, and use machine learning to adapt to the attack pattern. There are so many services offering this real time DDOS protection but for a price of \$20/month minimum.



Hardening Against CPU Excess Usage on Target 1

Patch Commands

- `sudo apt update && sudo apt -y upgrade` (Update/Upgrade Software)
- `sudo apt purge application` (Removing and Re-Installing apps)
- `sudo apt update`
- `sudo apt install application`

Some of the issue to high CPU usage can be related to not updated/upgraded software that might have new patches that make the software more efficient. Another problem could be improperly installed code. By using the patch above one can update all the system software. If this does not work then we can move on by uninstalling and reinstalling the given program, to see if the issue was a problem in the way it was originally installed.

Implementing Patches with Ansible

Playbook Overview

Ansible is an efficient way for patching multiple machines on a given network that have the same vulnerability.

As seen by the sudo code on the right, this is a general example on how to patch against high CPU usage.

```
---
- name: Configure vulnerability patch
  hosts: Target1
  remote_user: root
  become: true
  tasks:
    # Use apt module
    - name: Update Software
      apt:
        name: update

    # Use apt module
    - name: Upgrade Software
      apt:
        name: upgrade

    # Use apt module
    - name: Remove given application
      apt:
        name: purge
        command: purge "target app"

    # Use apt module
    - name: Install Software
      apt:
        name: install
        command: install "target app"
```