X-CORP

Network Analysis

Security Engineering: CSIRT Division

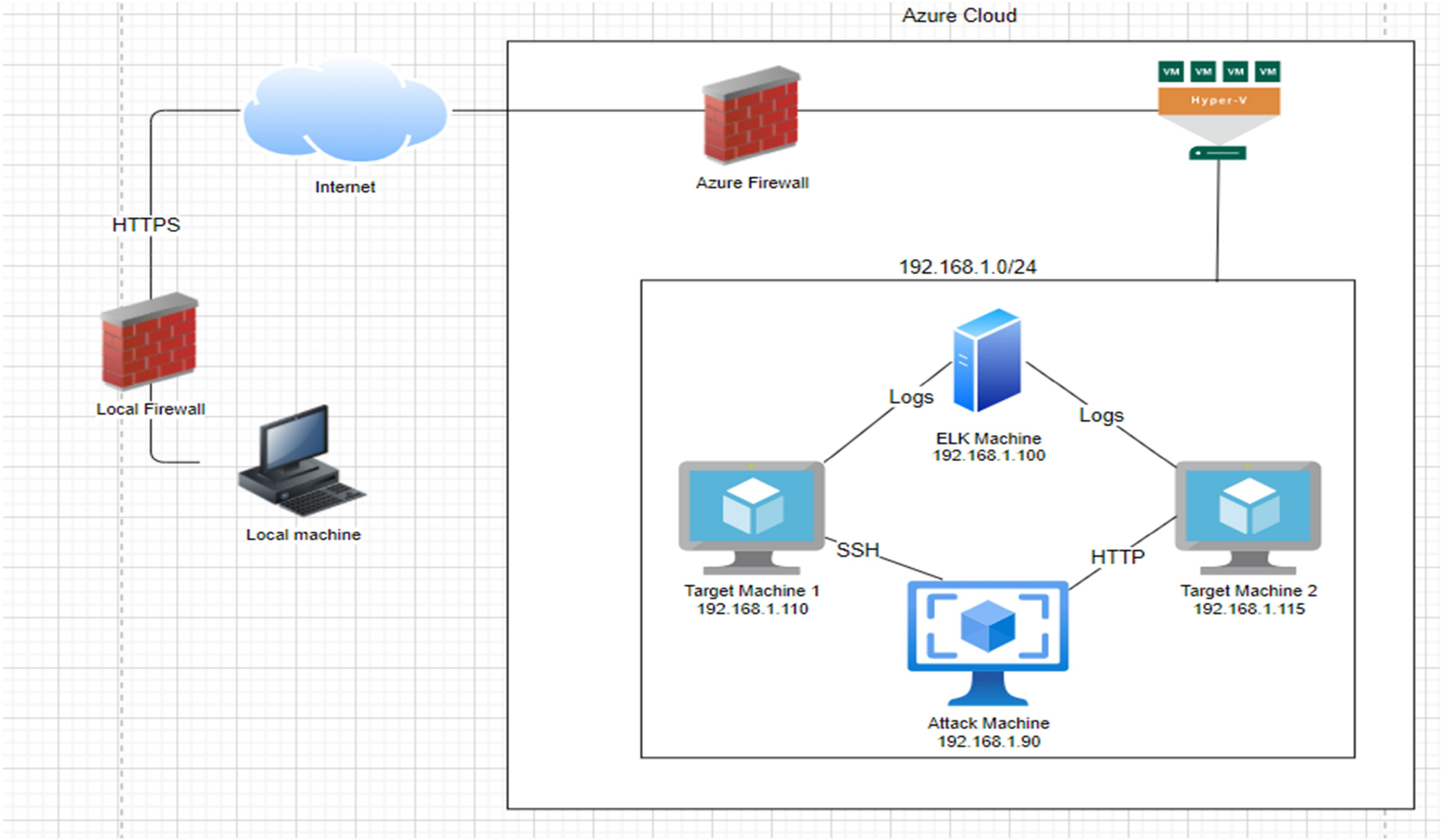
Attack, Defense & Analysis of X-CORP’S Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24 & 10.6.12.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1 & 10.6.12.0.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

Network Topology – Machines & Network

Network
Address Range:
192.168.1.0/24 & 10.6.12.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1 &
10.6.12.0.1

Machines

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

Machines

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 172.16.4.205
OS: Windows
Hostname: ROTTERDAM-PC

IPv4: 10.0.0.201
OS: Windows
Hostname: BLANCO-DESKTOP

Network
Address Range:
192.168.1.0/24 &
10.6.12.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1 &
10.6.12.0.1

Machines
IPv4: 172.16.4.205
OS: Windows
Hostname: ROTTERDAM-PC

IPv4: 10.0.0.201
OS: Windows
Hostname: BLANCO-
DESKTOP

Critical Vulnerabilities: Target 1

Assessment uncovered the following critical vulnerabilities in ***Target 1***.

Vulnerability	***Description***	***Impact***
Open Web Port (Port 80) CVE-2019-6579	Port 80 is commonly used for web communication and if left open and unsecure, it can allow public access.	Access to web server.
Unfiltered SSH Port (Port 22) CVE-2002-1715	Port 22, also known as the secure shell port, allows a user to remotely connect to another machine on a network via remote command execution.	SSH into target machine.
User Enumeration	Web application vulnerability that allows attackers to use bruteforce techniques to validate users on a network.	Enumerate a list of users.

Critical Vulnerabilities: Target 1

Assessment uncovered the following critical vulnerabilities in ***Target 1***.

Vulnerability	***Description***	***Impact***
Weak User Credentials	Short names, first name, or any simple combination.	Password is easy to obtain through social engineering.
Misconfigured Security Controls	Improper controls are implemented leaving systems vulnerable to exploits.	Allows unauthorized access.
Confidential Data Improperly Secured	Confidential data, such as user login information, is easily accessible with no security.	Database server configuration information easily accessible.
Trojan Malware	Malicious computer virus.	Malware downloaded locally and infected multiple hosts on network.

Critical Vulnerabilities: Target 2

Assessment uncovered the following critical vulnerabilities in ***Target 2***.

Vulnerability	***Description***	***Impact***
WordPress XML-RPC DOS	WordPress XML-RPC parsing is susceptible to DOS attacks by executing pingback.ping.	Several affected WordPress installations can launch a botnet level attack.
WordPress XML-RPC Ping	Using HTTP POST request smuggling to bypass front-end security controls.	Application's internal layers are targeted.
Cloudflare Protection Bypass	Execution of pingback.ping method can be used to bypass DNS level protection.	Target's public IP address revealed.

Traffic Profiles

Traffic Profile on 192.168.1.0/24

Analysis identified the following characteristics of the traffic on the network:

Feature	*Value*	*Description*
Top Talker (192.168.1.90)	Ip.addr==192.168.1.0/24	Machine that sent the most traffic.
Most Common Protocols (HTTP, SSH, TCP, UDP)	Ip.addr==192.168.1.0/24	Most common protocols on the network.
3 Unique IP Addresses (192.168.1.90, 192.168.110, 192.168.1.115)	Ip.addr==192.168.1.0/24	Count of observed IP addresses.
Subnets (255.255.255.0)	Ip.addr==192.168.1.0/24	Observed subnet ranges.

Traffic Profile on 10.6.12.0/24

Analysis identified the following characteristics of the traffic on the network:

Feature	*Value*	*Description*
Top Talkers (172.16.4.205), (185.243.115.84), (166.62.11.64)	Ip.addr==10.6.12.0/24	Machines that sent the most traffic.
Most Common Protocols (HTTP, TCP, UDP)	Ip.addr==10.6.12.0/24	Most common protocols on the network.
2 Unique IP Addresses (172.16.4.205 & 185.243.115.84)	Ip.addr==172.16.4.205 and 185.243.115.84	Count of observed IP addresses.
Subnets (255.255.255.0)	Ip.addr==10.6.12.0/24	Observed subnet ranges.
1 Malware Species (Trojan malware)	Ip.addr==10.6.12.203 and http.request.method==GET	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity:

"Normal" Activity

- Employees accessing public KB
- Employees checking emails

Suspicious Activity

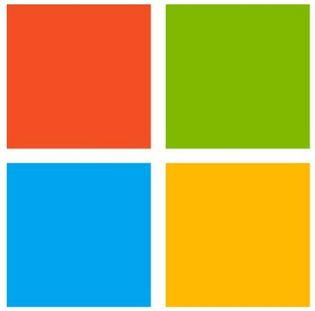
- Enumerating users – WPSCAN
- Executing pingback.ping command
- Accessing back-end DB server files – "wp.config.php" file
- Accessing DB servers and dumping hashes
- Setting up a private Active Directory Domain

Normal Activity

Normal Behavior – Accessing Public Knowledgebase

Knowledgebase Articles:

- HTTPS to establish a secure connection to Microsoft’s website.
- User accessed files on creating private domains.

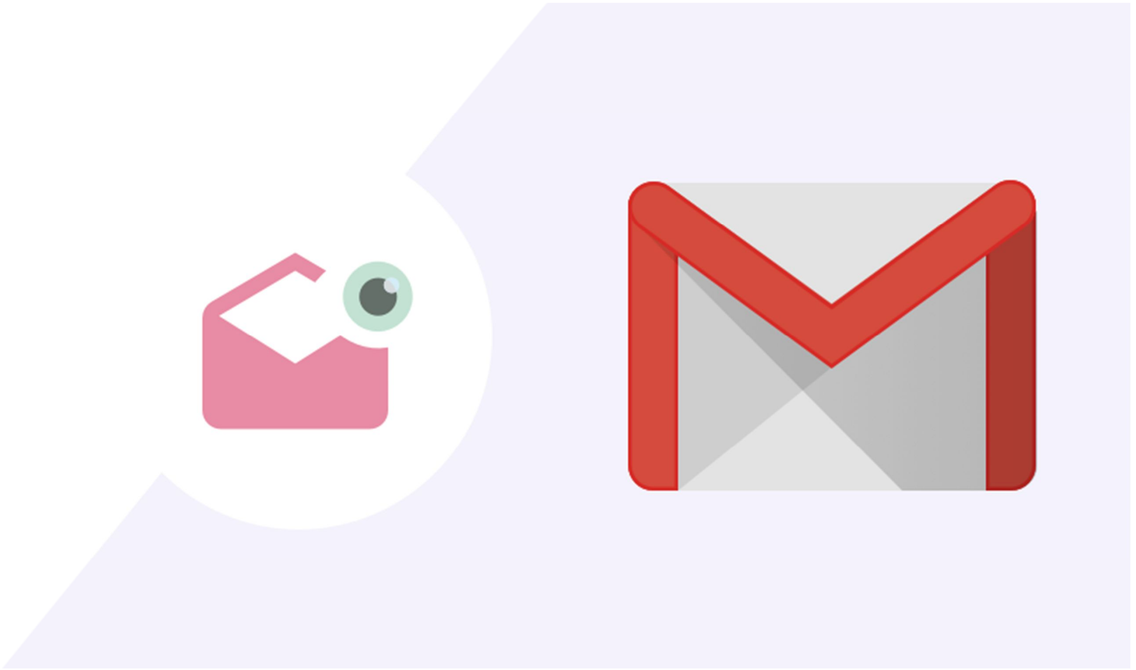


Microsoft

Name of Normal Behavior – Accessing Google Workspace

Accessing Email:

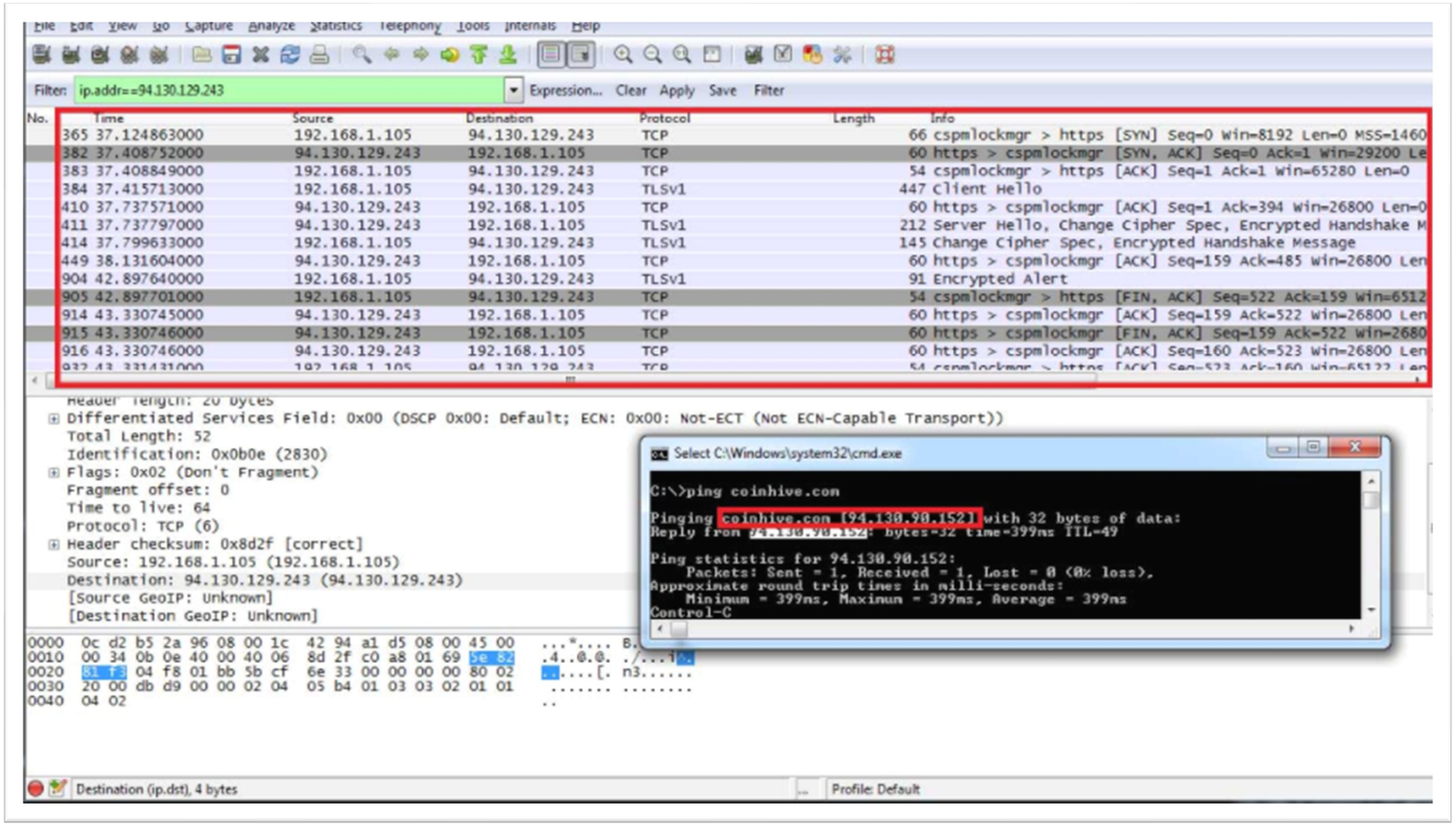
- HTTPS to establish a secure connection with the Google client
- Users authenticate to access email



Malicious Activity

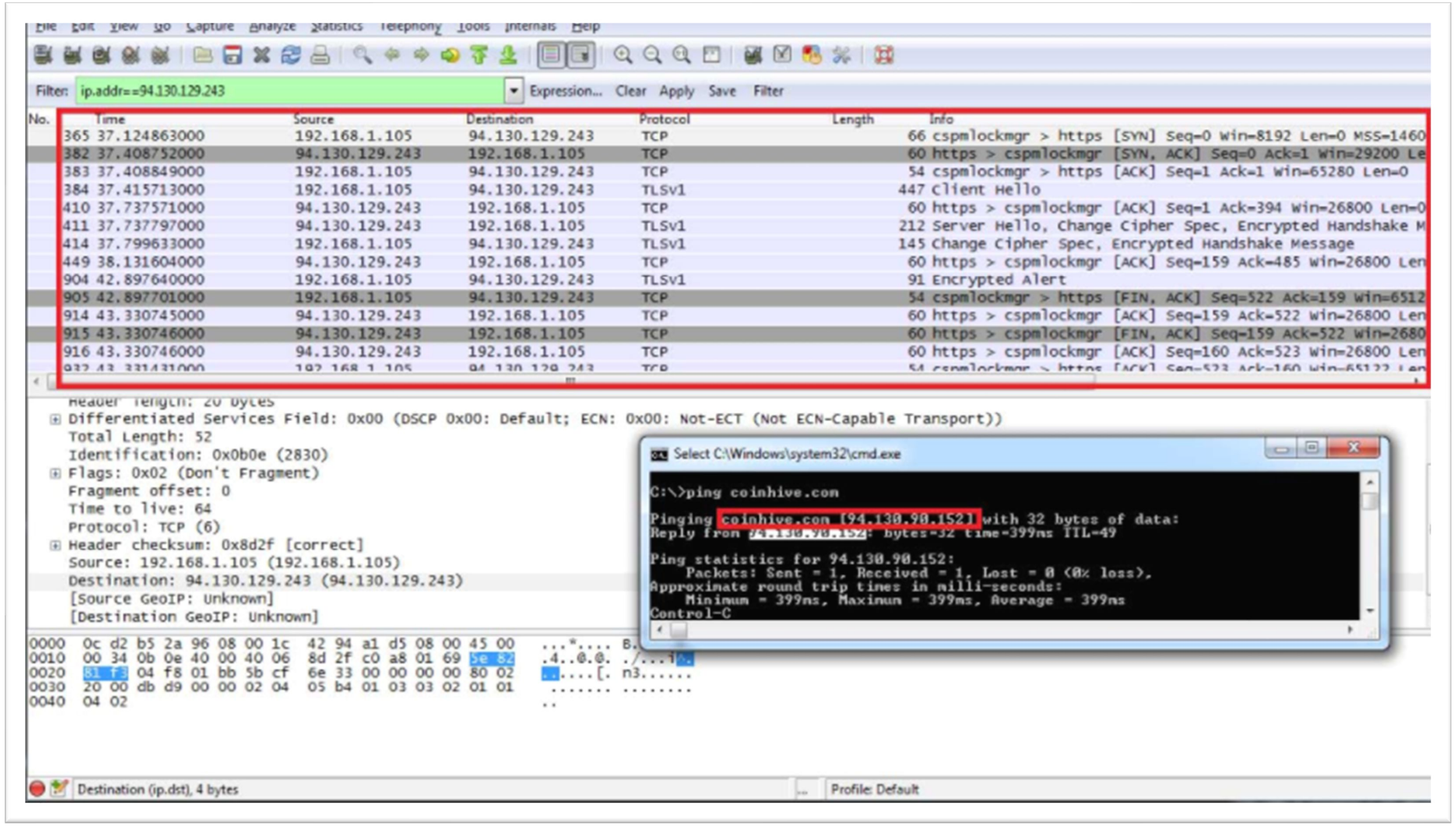
Malicious Behavior – Enumeration

- Excessive HTTP errors (400 errors)
- User ran a WPSCAN to enumerate potential users to target.
  - Enumeration is noisy



Malicious Behavior – XML-RPC Ping & DOS

- XML-RPC
- XML-RPC ping using HTTP POST smuggling to bypass front-end security controls
- Pingback.ping to bypass DNS level protection to launch a Cloudflare attack
    - Allowed for command & control – botnets



Malicious Behavior – Unauthorized Access & Dumping Hashes

- Improper implementation of security controls allows for exploitation
- SSH port 22 – Michael’s account to access SQL server
- User SSH wtih Michael’s discovered credentials to access SQL server to dump hashes

Malicious Behavior – Creating a Private Domain

- Private domain created on corporate network.
- Users were constantly browsing videos on YouTube
- Trojan Malware downloaded
  - Additional hosts infected
  - Hosts infected:
    - 10.6.12.203
    - 172.16.4.205
    - 185.243.115.84 – suspicious activity detected
    - 166.62.11.64

Malicious Behavior – Illegal Torrenting on Private Domain

- Users torrenting on network
  - Downloading copyrighted material
  - User downloaded recipe files
- Copyright Infringement
  - This creates some legal complications

Recommendations – System Hardening

Against Malware

- Implement an IDS/IPS
  - Real-time alerts to events
  - Protection from the network layer and up
- Utilize antivirus tools
  - Protects host from malicious programs

Recommendations – WordPress Service Hardening

Application Hardening

- Update WordPress Service
- Implement a load balancer
  - Filter requests made to web server
- Disable REST API
  - Prevents enumeration
- Implement proper security controls to servers & systems
  - Prevent unauthorized users from viewing sensitive information

Recommendations – Provisioning User Access

User Privileges, Rights Management, and IAM

- Implement least privilege
- Implement “zero trust”
- Set alerts for authentication logs
- Authentication, Authorization, and Accounting (AAA)

Recommendations – Implementing IDS/IPS

HIDS, NIDS, HIPS, and NIPS

- Host Intrusion Detection Systems (HIDS)
  - Monitors and detects malicious activity on ***HOST.***
- Network Intrusion Detection Systems (NIDS)
  - Monitors and detects malicious activity on ***NETWORK.***
- Host Intrusion Prevention Systems (HIPS)
  - Protects ***HOST*** from malicious attacks from layer 3 to 7.
- Network Intrusion Prevention Systems (NIPS)
  - Protects ***NETWORK*** from malicious attacks.

Recommendations – Employee Training

Corporate Policy & Laws

- Train employees on technology usage & privileges
- Employee training on corporate policies, regulations, and laws.
- Best practices (ITIL, COBIT, etc.)

The End