X-CORP
Blue Team: Log Analysis & Attack Characterization

Security Engineering: CSIRT Division

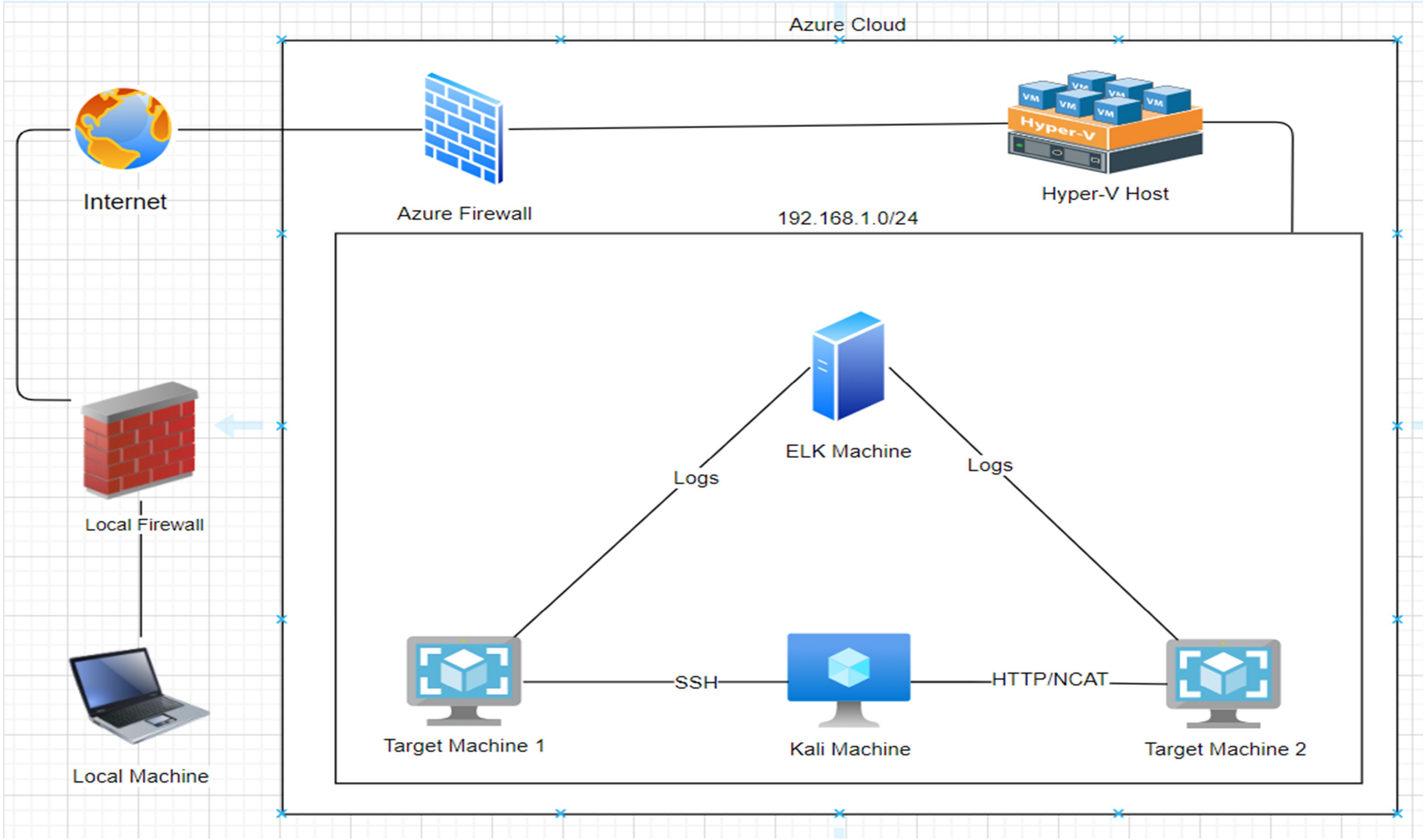
Attack, Defense, and Analysis of X-CORP’S Network

Table of Contents – Blue Team

This document contains the following resources:

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: 192.168.1.90
OS: Linux
Hostname: Kali Machine

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK Machine

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Hyper-V ML-REFVM-684427	192.168.1.1	Host Machine
Kali	192.168.1.90	Attack Machine
Target Machine 1	192.168.1.110	Target Machine
Target Machine 2	192.168.1.115	Second target machine
ELK	192.168.1.100	ELK machine that hosts Kibana & Elasticsearch Watcher

Critical Vulnerabilities: Target 1

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

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

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

Alerts Implemented

Excessive HTTP Errors Alert

- Metric: WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- Threshold: 400
- Vulnerability Mitigated: Bruteforce & Enumeration
- Reliability: Alert is highly reliable

HTTP Request Size Monitor Alert

- Metric: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- Threshold: 3500
- Vulnerability Mitigated: XSS, DDOS, Directory Traversal
- Reliability: Alert is reliable, but can generate false positives

CPU Usage Monitor Alert

- Metric: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- Threshold: 0.5
- Vulnerability Mitigated: Malware & Viruses
- Reliability: Alert is highly reliable

Hardening

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
- ELK Stack
  - Configure ELK stack and install beats to monitor changes to metrics & logs

Recommendations – WordPress Service Hardening

Application Hardening

- Update WordPress Service
- Implement a load balancer
  - Distributes traffic
  - Optimizes resources & response
  - Filter requests made to web server
- Disable REST API
  - Prevents enumeration
- Implement proper security controls to servers, systems, and applications
  - Prevent unauthorized users from accessing sensitive, confidential, critical, and proprietary information

Recommendations – Provisioning User Access & Security

User Privileges, Rights Management, and IAM

- Implement least privilege
- Implement “zero trust”
- Implement SSO
- Baselines for secure configuration & operations
  - What should be under direct control?
- Secure network (i.e., DMZ, air-gaps, isolation, and segmentation, etc.)
- Set alerts for authentication logs
  - Anomalies & unauthorized access
- 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 & Awareness

Corporate Policies, Laws, and Frameworks

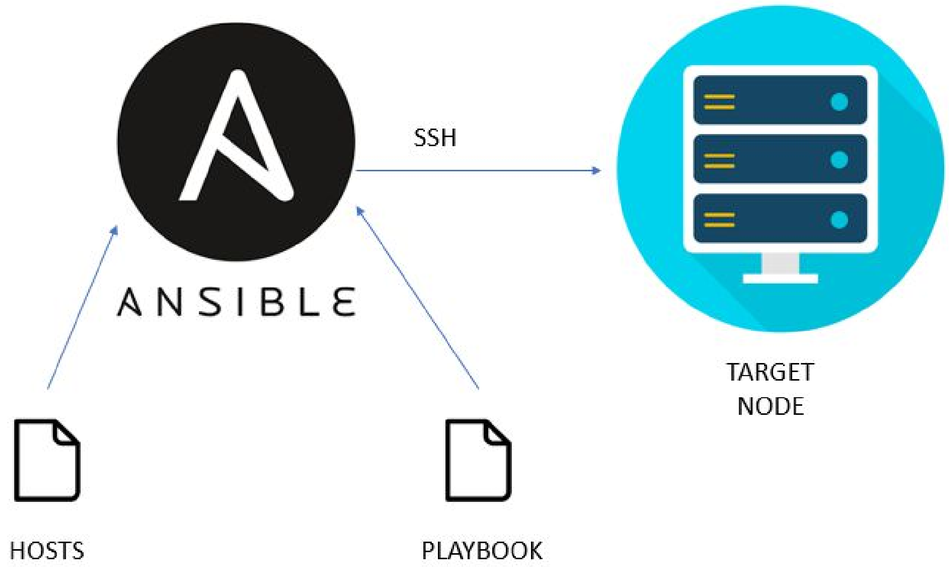
- Train employees on technology usage & privileges
- Employee training on corporate policies, regulations, and laws.
- Best practices (i.e., ITIL, COBIT, ISO, NIST, etc.)
- Compliance & Regulations (i.e., SOX, HIPAA, PCI, GDPR, Data Privacy Act, etc.)
- Auditing & Compliance

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

- WordPress Patch – wordpress.yml
  - Playbook file backups and archives data
  - Installs latest version of WordPress
- ELK Stack – elk.yml
  - Configures ELK with docker
  - Use ELK to monitor activity
- Beats
  - Filebeat – helps collect file logs
  - Metricbeat – collects system metrics
  - Packetbeat – helps with packet analysis



The End