# **Blue Team: Summary of Operations**

**Table of Contents**

## Network Topology

## Description of Targets

## Monitoring the Targets

## Patterns of Traffic & Behavior

## Suggestions for Going Further

**Network Topology**

The following machines were identified on the network:

* Name of VM 1: Target1
  + Operating System: Linux 3.X|4.X
  + Purpose: Web Server - Vulnerable VM
  + IP Address: 192.168.1.110
* Name of VM 2: Kali
  + Operating System: Linux 2.6.32
  + Purpose: Pen Testing Machine
  + IP Address: 192.168.1.90
* Name of VM 3: Capstone
  + Operating System: No exact OS Match but appears to be Linux
  + Purpose: Alert Testing Machine
  + IP Address: 192.168.1.105
* Name of VM 4: ELK
  + Operating System: No exact OS Match but appears to be Linux
  + Purpose: Gathers Logs and Alerts: Elasticsearch, Logstash, Kibana
  + IP Address: 192.168.1.100
* Name of VM 5: Target2
  + Operating System: Linux 3.X|4.X
  + Purpose: Web Server - Vulnerable VM
  + IP Address: 192.168.1.115

**Description of Targets**

The target of this attack was: Target 1: 192.168.1.110

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

**Monitoring the Targets**

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

**Name of Alert 1**

Alert 1: HTTP Errors Alert:

Implemented as follows:

* Metric: HTTP Status Errors
* Threshold: Above 400 over 1 minute
* Vulnerability Mitigated: Brute Force Attacks
* Reliability: High: Provides critical data against Brute Force Attacks

**Name of Alert 2**

Alert 2: Failed SSH Password Attempts:

Implemented as follows:

* Metric: system.auth.ssh.method
* Threshold: Above 5 over the last 5 minutes
* Vulnerability Mitigated: Unwarranted SSH Login Attempts
* Reliability: High: Provides data to make sure unauthorized users aren't trying to SSH into the network

**Name of Alert 3**

Alert 3: Port Scan:

Implemented as follows:

* Metric: source.port
* Threshold: Above 2000 over the last 5 minutes
* Vulnerability Mitigated: Port Scanning - to see what ports are open on the network
* Reliability: High: Important to know if people are scanning your network for open ports and vulnerabilities

**Name of Alert 4**

Alert 3: Sudo Commands Alert:

Implemented as follows:

* Metric: system.auth.sudo.error
* Threshold: Above 1 over the last 5 minutes
* Vulnerability Mitigated: Catching a User trying to access restricted folders or gain root privileges
* Reliability: High: An attacker using sudo or gaining root access can have irreversible effects. There is a slight chance of false alerts due to user accidents - but users should know their access and what they can view

**Name of Alert 5**

Alert 3: CPU Usage Monitor:

Implemented as follows:

* Metric: system.process.cpu.total
* Threshold: Above .5 over the last 5 minutes
* Vulnerability Mitigated: DDoS Attacks
* Reliability: Medium - High: Keeping our network up and running by allowing normal traffic and speeds is important

Suggestions for Going Further:

Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain *how* to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

* Vulnerability 1: Brute Force Attack
  + Patch: Set up a whitelist of IP addresses or range.
  + Why It Works: This will block any unwanted IP's from trying to login and you are restricting access to only the IP's you know.
* Vulnerability 2: Failed SSH Password/Login Attempts
  + Patch: Set up key-based logins with ssh-keygen
  + Why It Works: This is a much more secure connection and users can have a private key and passphrase.
* Vulnerability 3: Port Scan
  + Patch: Install a Firewall and Internal auditing
  + Why It Works: Firewalls will detect port scans in progress and shut them down. Also, internal audits are always important. These will make sure you are checking your network periodically to make sure you do not have any weak points out in the public.
* Vulnerability 4: Sudo Commands
  + Patch: Limit access to sudo privileges and conduct audits on sudoers folder
  + Why It Works: Limiting who has access to run sudo will prevent unnecessary privileges. It is also important to monitor the sudoers folder periodically to ensure users who do not belong do not have access to sudo rights.
* Vulnerability 5: DDos Attack
  + Patch: Install a Web Application Firewall (WAF)
  + Why It Works: A WAF helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as: cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.

# 

# 

# 

# 

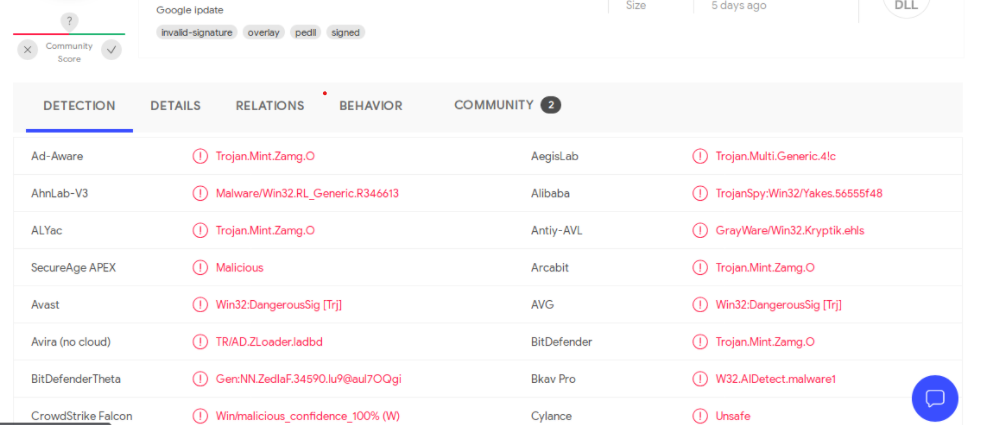
# **Network Forensic Analysis Report**

## **Time Thieves**

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?  
   frank-n-ted.com
2. What is the IP address of the Domain Controller (DC) of the AD network?  
   10.6.12.12
3. What is the name of the malware downloaded to the 10.6.12.203 machine?  
   June11.dll

Once you have found the file, export it to your Kali machine's desktop.

4. 

5. What kind of malware is this classified as?  
This is classified as a Trojan

## **Vulnerable Windows Machine**

1. Find the following information about the infected Windows machine:
   * Host name: Rotterdam-PC
   * IP address: 172.16.4.205
   * MAC address: 00:59:07:b0:63:a4
2. What is the username of the Windows user whose computer is infected?  
   matthijs.devries
3. What are the IP addresses used in the actual infection traffic?  
   31.7.62.214  
   185.243.115.84
4. As a bonus, retrieve the desktop background of the Windows host.

## **Illegal Downloads**

1. Find the following information about the machine with IP address 10.0.0.201:
   * MAC address: 00:16:17:18:66:c8
   * Windows username: Blanco
   * OS version: Windows NT
2. Which torrent file did the user download? Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent **Path**

# **Red Team: Summary of Operations**

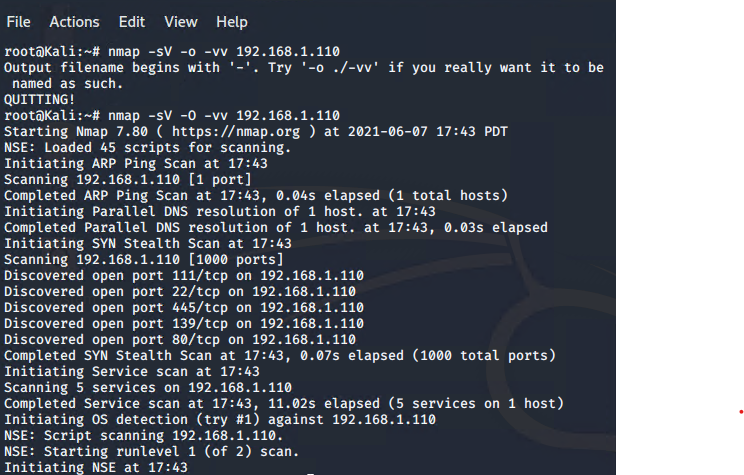
Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

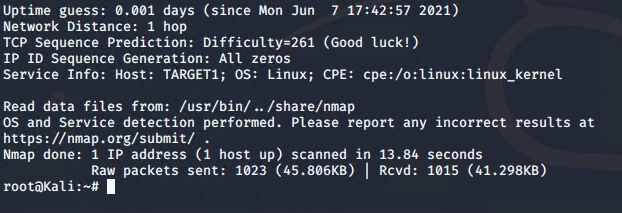
Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

## **nmap -sV -O -vv 192.168.1.110**



## 



This scan identifies the services below as potential points of entry:

* Target 1
  + Port 22/tcp - ssh - Open
  + Port 80/tcp - http - Open
  + Port 111/tcp - rbcbind - Open
  + Port 139/tcp - netbios-ssn - Open
  + Port 445/tcp - netbios-ssn - Open

Port 22

An open port 22 can allow ssh logins. Keeping port 22 open usually welcomes attackers to brute force using a dictionary attack.

Port 80

Port 80 allows for HTTP traffic. Attackers can also use brute force and dictionary attacks to gain access.

Port 111

Port 111 allows attackers to see what services are running. This can be used for reconnaissance activity. The RPC Service has a history of security vulnerabilities.

Port 139 & 445

These ports allow for network file sharing. Also allow the potential of a possible reverse shell via Metasploit.

The following vulnerabilities were identified on each target:

### **Critical Vulnerabilities**

The following vulnerabilities were identified on each target:

Target 1

1. User Enumeration (WordPress site)
2. Weak User Password
3. Unsalted User Password Hash (WordPress database)
4. Misconfiguration of User Privileges/Privilege Escalation

### **Explotation**

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

Target 1

* Flag1: b9bbcb33ellb80be759c4e844862482d
* Exploit Used:
  + WPScan to enumerate users of the Target 1 WordPress site
  + Command:
    - $ wpscan --url http://192.168.1.110 --enumerate u