NETWORK ANALYSIS TEAM SUMMARY OF OPERATIONS

MONITORING, ANALYSIS AND MITIGATION

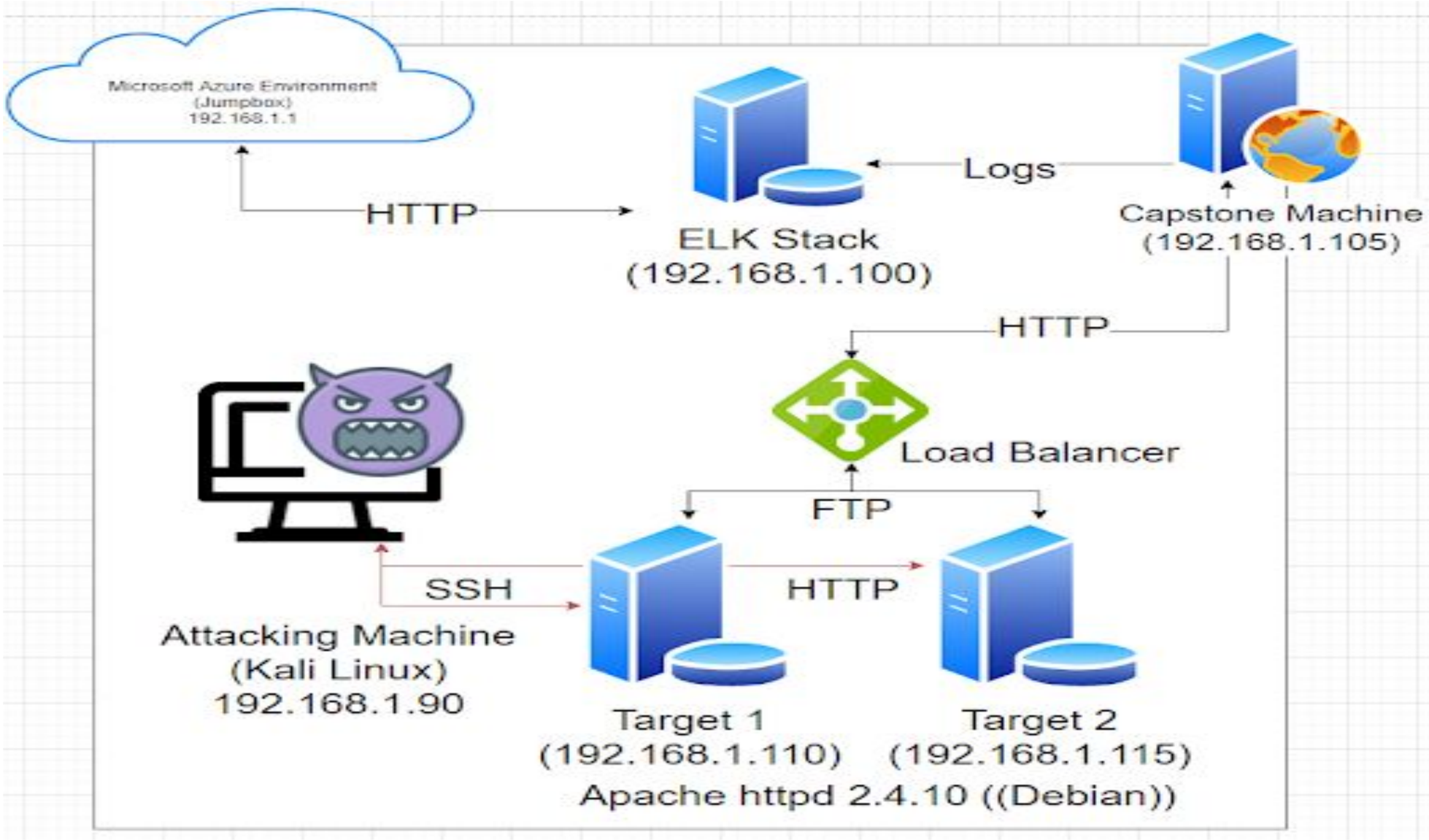
OF A VULNERABLE NETWORK

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.1/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Linux Kali 5.4.0-kali3
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu 18.04.4 LTS
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.04.4 LTS
Hostname: ELK

IPv4: 192.168.1.110
OS: debian 3.16.0-6-amd64
Hostname: Target 1

IPv4: 192.168.1.115
OS: debian 3.16.0-6-amd64
Hostname: Target 2

Critical Vulnerabilities: Target 1 & 2

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

Vulnerability	Description	Impact
Port 22	ssh	With the correct credentials is able to access network
Port 111	rpc-bind	Is used for PortMapping and is always listens on TCP/UDP.
Port 139	netbios-ssn	An attacker is able to run NBSAT a diagnostic tool over TCP/IP
Port 445	netbios-ssn	Is the preferred Port for Windows FileSharing and numerous other services

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 - 45 million bytes 185.243.115.84 - 26 million bytes 166.62.111.64 - 16 million bytes	Machines that sent the most traffic.
Most Common Protocols	UDP - 11697 packets TCP - 92280 packets TLS - 7272 packets	Three most common protocols on the network.
# of Unique IP Addresses	30 unique addresses discovered	Count of observed IP addresses.
Subnets	172.16.4.0/24	Observed subnet ranges.
# of Malware Species	55	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

- Watching Youtube
- Web Browsing

Suspicious Activity

- Downloading Torrents for Illegitimate Purposes
- Downloading Malware

Normal Activity

[Watching Youtube]

- Two users set up a private web server on the corporate network. Their IPs are on the 10.6.12.0/24 network range. SMB2 traffic, HTTP, Browser
- The employee in question was watching Youtube during work hours using an unauthorized domain controller.
- Include screenshots of packets justifying your conclusions.

10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com SRV 0
10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.12.12

- The IP of the Domain Controller is 10.6.12.12

[Web Browsing]

Summarize the following:

- HTTP protocol
- We can see that the IP user of 172.16.4.205 is browsing blog under http://mysocalledchaos.com
- The IP user is taking in a lot of .png picture files to print out for sticker use

```
▸ Frame 3983: 405 bytes on wire (3240 bits), 405 bytes captured (3240 bits) on interface eth0, id 0
▸ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
▾ Internet Protocol Version 4, Src: 172.16.4.205, Dst: 166.62.111.64
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 391
    Identification: 0x01ce (462)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x3147 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.4.205
    Destination: 166.62.111.64
▸ Transmission Control Protocol, Src Port: 49190, Dst Port: 80, Seq: 1765, Ack: 61528, Len: 351
▾ Hypertext Transfer Protocol
  ▾ GET /wp-content/plugins/instagram-feed/js/sb-instagram.min.js?ver=1.10.1 HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /wp-content/plugins/instagram-feed/js/sb-instagram.min.js?ver=1.10.1 HTTP/1.1\r\n]
      Request Method: GET
    ▸ Request URI: /wp-content/plugins/instagram-feed/js/sb-instagram.min.js?ver=1.10.1
      Request Version: HTTP/1.1
  Host: mysocalledchaos.com\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
  Accept: */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Connection: keep-alive\r\n
  Referer: http://mysocalledchaos.com/\r\n
  \r\n
  [Full request URI: http://mysocalledchaos.com/wp-content/plugins/instagram-feed/js/sb-instagram.min.js?ver=1.10.1]
  [HTTP request 6/14]
  [Prev request in frame: 3848]
  [Response in frame: 4086]
  [Next request in frame: 4087]
```

Malicious Activity

[Downloading Torrents]

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)? Typical traffic that was observed was search requests and typical keep connection alive. The Protocols observed were TCP, HTTP
- What, specifically, was the user doing? Which site were they browsing? Etc. The user in question was downloading a Torrent. Not authorized by the company as it breaks copyright laws. http://files.publicdomaintorrents.com
- Include screenshots of packets justifying your conclusions.

- Include a description of any interesting files.

The video file in question was Betty_Boop_Rhythm_on_the_Reservation.avi

[Downloading Malware]

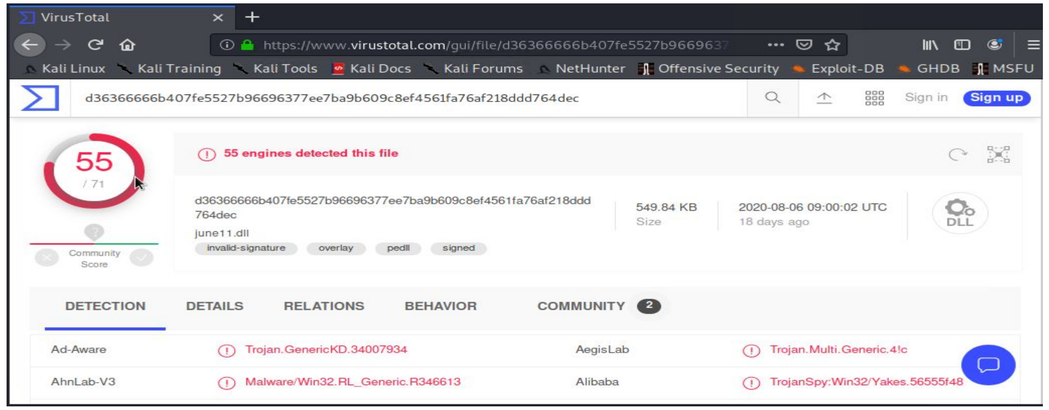
Summarize the following:

- What kind of traffic did you observe? Which protocol(s)? TCP and HTTP
- What, specifically, was the user doing? Which site were they browsing? Etc. From the data we retrieved it appears the employee was browsing and was redirected to a malicious webpage.

```
58752 2020-06-30 13:04:39 LAPTOP-5WKHX9YG.fra… 205.185.125.104      HTTP      312 GET /files/june11.dll HTTP/1.1
58759 2020-06-30 13:04:39 LAPTOP-5WKHX9YG.fra… 205.185.125.104      TCP        54 49739 → http(80) [ACK] Seq=480
```

- Include a description of any interesting files.

The malware in question was june11.dll which is a Trojan.



The End