## Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

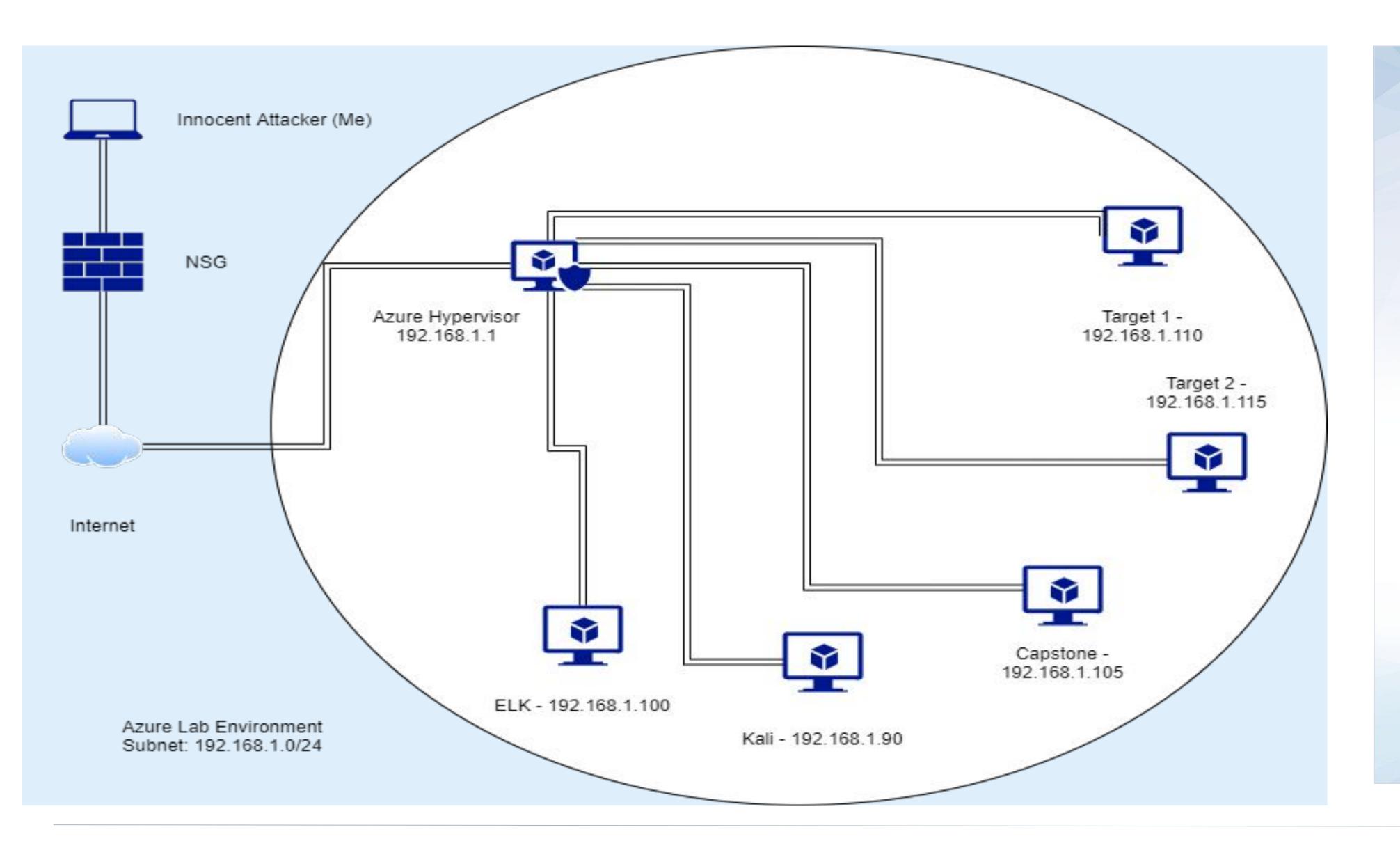
### **Table of Contents**

This document contains the following resources:



## Network Topology & Critical Vulnerabilities

## **Network Topology**



#### Network

Address Range: 192.168.1.0/24 Netmask: 1

Gateway: 255

#### **Machines**

IPv4: 192.168.1.90

OS: Linux

Hostname: Kali

IPv4: 192.168.1.100

OS: Linux

Hostname: ELK

IPv4: 192.168.1.110

OS: Linux

Hostname: Target 1

IPv4: 192.168.1.115

OS: Linux

Hostname: Target 2

## 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/ 182.243.115.84/10.0.0.201	Machines that sent the most traffic.	
Most Common Protocols	HTTP/SMB2/SMBA(AD)	Three most common protocols on the network.	
# of Unique IP Addresses	804	Count of observed IP addresses.	
Subnets	172.168.4.0/24/10.0.0/24/192. 168.1.0/24	Observed subnet ranges.	
# of Malware Species	1identified _trojan "june11.dll"	Number of malware binaries identified in traffic.	

## **Behavioral Analysis**

#### Purpose of Traffic on the Network

Web browsing

#### "Normal" Activity

Youtube, web browsing, web application usage (skype etc)

#### **Suspicious Activity**

Downloading malware, torrenting, sandboxing, and using cloud servers

# Normal Activity

## [Name of Normal Behavior 1]

- What kind of traffic did you observe? Which protocol(s)? HTTP / TCP / DNS traffic
- What, specifically, was the user doing? Which site were they browsing? Etc.
  - o Browsing websites, reading Angie's blogs, trying to jailbreak their iphone

```
HTTP Requests by HTTP Host
   www.vinylmeplease.com
   www.sabethahospital.com

    www.publicdomaintorrents.com

       /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
 www.msftncsi.com
 www.iphonehacks.com
       /wp-includes/js/wp-embed.min.js
       /wp-includes/js/jquery/jquery-migrate.min.js
       /wp-includes/js/comment-reply.min.js
       /wp-includes/css/dist/block-library/style.min.css
       /wp-content/themes/iphonehacks/style.css?ver=1.130
       /wp-content/themes/iphonehacks/js/modernizr.js
       /wp-content/themes/iphonehacks/js/jquery.fitvids.js
       /wp-content/themes/iphonehacks/js/foundation.min.js
       /wp-content/themes/iphonehacks/js/app.js
       /wp-content/themes/iphonehacks/img/menu.png
       /wp-content/themes/iphonehacks/img/logo.jpg
       /wp-content/themes/iphonehacks/fonts/fontawesome-webfont.woff2?v=4.6.3
       /wp-content/themes/iphonehacks/favicon.png
       /wp-content/themes/iphonehacks/favicon.ico
       /wp-content/themes/iphonehacks/css/style.css
       /wp-content/themes/iphonehacks/css/font-awesome.min.css
```

```
ocsp.digicert.com
mysocalledchaos.com
   /wp-includes/js/wp-emoji-release.min.js?ver=5.2.2
   /wp-includes/js/wp-embed.min.js?ver=5.2.2
   /wp-includes/js/masonry.min.js?ver=3.3.2
   /wp-includes/js/jquery/jquery.masonry.min.js?ver=3.1.2b
   /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp
   /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1
   /wp-includes/js/imagesloaded.min.js?ver=3.2.0
   /wp-includes/css/dist/block-library/style.min.css?ver=5.2.2
   /wp-includes/css/dashicons.min.css?ver=5.2.2
   /wp-content/uploads/useanyfont/uaf.css?ver=1524058848
   /wp-content/uploads/2019/04/MomLifeStickers-Feat-400x600.png
   /wp-content/uploads/2019/03/Financial-Planner-stickers-feat-400x600.jpg
   /wp-content/uploads/2019/02/HomeandGardenStickers3-400x600.png
   /wp-content/uploads/2019/01/2019GoalsADHD-400x600.jpg
   /wp-content/uploads/2018/11/AdventCalendarFillers-400x600.jpg
   /wp-content/uploads/2018/11/12-Days-of-Christmas-Swap-400x600.jpg
   /wp-content/uploads/2018/02/self-care.jpg
   /wp-content/uploads/2018/02/photography.jpg
   /wp-content/uploads/2018/02/footer-218x300.png
   /wp-content/uploads/2018/02/fleshy-in-this-2571786.jpg
   /wp-content/uploads/2018/02/cropped-MSCC header 2018-1.png
```

### [Name of Normal Behavior 2]

- What kind of traffic did you observe? HTTP, TCP, and DNS traffic Which protocol(s)?
  - Most packets in top 3 categories include: HTTP, TCP, & DNS traffic
- What, specifically, was the user doing? Which site were they browsing? Etc.
  - Interestingly Roger spent quite some time using Amazon CloudFront and Youtube

No		Time	Source	Destination	Protocol	Length Info
1	13625	156.464426600	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.1	TCP	1411 80 → 50233 [ACK] Seq=3266 Ack=1229 Win=32
+	13624	156.441852200	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.1	HTTP	74 HTTP/1.1 200 OK (PNG)
	13623	156.440671500	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.1	TCP	1411 80 → 50234 [ACK] Seq=9514 Ack=1628 Win=33
	13622	156.418095600	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.1	TCP	1411 80 - 50234 [ACK] Seq=8169 Ack=1628 Win=33
	13621	156.395562800	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.1	TCP	1411 80 - 50234 [ACK] Seq=6824 Ack=1628 Win=33
	13618	156.362560100	www-googletagmanager.l.google.com	Roger-MacBook-Pro.1	TCP	74 443 → 50241 [SYN, ACK] Seq=0 Ack=1 Win=60
	13614	156.358231000	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.1	HTTP	208 HTTP/1.1 200 OK (PNG)
1	13613	156.354889400	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.1	TCP	1411 80 → 50231 [ACK] Seq=49376 Ack=1605 Win=3
1	13612	156.332299300	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.1	TCP	1411 80 → 50231 [ACK] Seq=48031 Ack=1605 Win=3
1	13611	156.309718100	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.1	TCP	66 80 → 50232 [ACK] Seq=132253 Ack=1696 Win=
	13609	156.307420800	youtube-ui.l.google.com	Roger-MacBook-Pro.1	TCP	66 443 → 50225 [ACK] Seq=75283 Ack=1345 Win=
1	13602	156.270954000	youtube-ui.l.google.com	Roger-MacBook-Pro.1	TLSv1.3	1213 Application Data, Application Data, Appli
1	13599	156.249437600	youtube-ui.l.google.com	Roger-MacBook-Pro.1	TLSv1.3	1411 Application Data [TCP segment of a reasse
1	13597	156.225803600	youtube-ui.l.google.com	Roger-MacBook-Pro.1	TLSv1.3	1411 Application Data [TCP segment of a reasse
1	13595	156.202174100	youtube-ui.l.google.com	Roger-MacBook-Pro.1	TLSv1.3	1411 Application Data [TCP segment of a reasse
1	13594	156.179593900	youtube-ui.l.google.com	Roger-MacBook-Pro.1	TLSv1.3	1411 Application Data [TCP segment of a reasse
1	13590	156.153854100	youtube-ui.l.google.com			1411 Application Data [TCP segment of a reasse
1	13589	156.131278800	youtube-ui.l.google.com	Roger-MacBook-Pro.1	TLSv1.3	1411 Application Data [TCP segment of a reasse
1	13588	156.108727500	youtube-ui.l.google.com	Roger-MacBook-Pro.1	TLSv1.3	1411 Application Data [TCP segment of a reasse

# Malicious Activity

### [Name of Malicious Behavior 1]

- What kind of traffic did you observe? Which protocol(s)?
  - Most malicious activity found used TCP and HTTP traffic in large quantities
- What, specifically, was the user doing? Which site were they browsing? Etc.
  - An infected user's computer upon download of malicious payload began communication with attacker site in spades as an outward indicator of trojan infection

No.	Time	Source	Destination	▲ Protocol	Length Info			
83589	855.591831900	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	HTTP	341 [TCP	Spurious Retransmissi	Lon] HT	
83588	855.586357800	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	54 80 →	49249 [ACK] Seq=22776	55 Ack=	
83587	855.585498000	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	54 80 →	49249 [ACK] Seq=22776	55 Ack=	
83583	855.569707500	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	ion] 80	
83581	855.546083800	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	Lon] 80	_
83580	855.523498500	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1199 [TCP	Spurious Retransmissi	Lon] 80	
83579	855.504316400	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	54 80 →	49249 [ACK] Seq=22662	20 Ack=	
83578	855.503466800	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	ion] 80	
83577	855.480909100	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	Lon] 80	
83576	855.458327500	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	Lon] 80	
83575	855.435729000	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	Lon] 80	
83574	855.413156300	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	ion] 80	
83573	855.390576500	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	ion] 80	
83571	855.367040100	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	Lon] 80	
83569	855.343504600	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	Lon] 80	
83566	855.319035400	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	ion] 80	
		b5689023.green.mattingsolutions		TCP	1411 [TCP	Spurious Retransmissi	Lon] 80	
83559	855.269057700	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	Lon] 80	
83558	855.246473400	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP	Spurious Retransmissi	Lon   80	

## [Name of Malicious Behavior 2]

- What kind of traffic did you observe? Which protocol(s)? HTTP / TCP
- What, specifically, was the user doing? Which site were they browsing? Etc.
  - After being infected with trojan, it appears user attempted to isolate infected files using online sandbox site ball.dardavies.com and while waiting for results he was visiting Angie's public blog at mysocalledchaos.com

No.		Time	Source	Destination	Protocol	Length Info
1	73200	721.163016600	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54 443 - 49236 [FIN, ACK] Seq=20525
1	73199	721.162276800	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 - 49239 [FIN, ACK] Seq=74841
1	73198	721.161450000	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54 443 → 49236 [ACK] Seq=20525 Ack=
100	73197	721.160431600	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	TCP	1411 [TCP Spurious Retransmission] 80
	73196	721.137845700	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 - 49244 [FIN, ACK] Seq=16499
1	73193	721.135067200	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 → 49238 [FIN, ACK] Seq=6414 A
1	73192	721.134203700	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 → 49243 [FIN, ACK] Seq=16511
1	73190	721.132389600	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 - 49240 [FIN, ACK] Seq=13557
	73189	721.131519200	b5689023.green.mattingsolutions	Rotterdam-PC.mind-hammer.net	HTTP	1411 [TCP Spurious Retransmission] Co
1	73186	721.107035100	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 → 49242 [FIN, ACK] Seq=15919
1	73185	721.106155000	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 → 49245 [FIN, ACK] Seq=16623
1000	73182	721.103399700	locprod1-elb-eu-west-1.prod.moza	Rotterdam-PC.mind-hammer.net	TCP	54 443 → 49193 [FIN, ACK] Seq=3786
1	73181	721.102528400	locprod1-elb-eu-west-1.prod.moza	Rotterdam-PC.mind-hammer.net	TLSv1.2	85 Encrypted Alert
1	73180	721.101140900	locprod1-elb-eu-west-1.prod.moza	Rotterdam-PC.mind-hammer.net	TCP	54 443 - 49193 [ACK] Seq=3755 Ack=1
Elle	73179	721.100277000	click.clickanalytics208.com	Rotterdam-PC.mind-hammer.net	TCP	54 443 - 49220 [FIN, ACK] Seg=13872
1	73178	721.099412700	click.clickanalytics208.com	Rotterdam-PC.mind-hammer.net	TCP	54 443 → 49220 [ACK] Seq=13872 Ack=
I	73176	721.097608300	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 - 49199 [FIN, ACK] Seq=815228
1	73173	721.094810200	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 → 49201 [FIN, ACK] Seq=205058
1	73172	721.093948100	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	54 80 → 49202 [FIN, ACK] Seq=913488

