Project 2, 3 IDS, honeypot NTOP

DV1591

Adrian Adborn, Viktor Listi, Moa Prim

Examinator: Oleksii Baranovskii and Anders Carlsson
Date: 2024-03-03

Introduction

For this report we have set up a functioning network containing two computers, a switch and a router. Honeypots were set up in virtual machines to attract suspicious traffic They were placed within the network to appear as valuable targets for potential attackers, which then the collected traffic was analyzed. The purpose of the assignment was to get a more realistic viewpoint on how a malware attack works, how easy it is to be attacked and what to do to prevent an attack from happening.

System Description

Our network was configured with two primary objectives 1. to mimic a small segment of a realistic network environment and 2. to capture and analyze malicious traffic using honeypots. This setup was essential for attracting and studying the real nature of attacks that a network could face in a real-world scenario.
The operating system for the monitoring computer was Security Onion Eval and for the other computer it was Ubuntu 22.04.4 LTS. The span configuration was implemented to mirror all network traffic to the Security Onion eval system. This enables traffic analysis and monitoring without interfering with the network's operational traffic flow. The management of our network and its security components was centralized through a dedicated interface on the Security Onion eval system. This resulted in the possibility of traffic analysis and threat detection.

System Information

Address space - 193.11.189.0-7 / 29
193.11.189.1 - Internal router
193.11.189.2 - Honeypot host PC
193.11.189.3 - Management interface for Security Onion Eval system
f0/2 (switch to PC) - Span interface for Security Onion Eval system
193.11.189.4 - 2 Honeypots in VM1, Metasploitable 2 in VM2.
193.11.189.10 - External router.

HoneyPots

The honeypots ran in vms on host 193.11.189.2 and networked through a bridge.

Apache

IP: 193.11.189.4
Port: 8080
Running: 2024/02/13 - 2024/03/03
Source : https://github.com/bocajspear1/honeyhttpd
Description:
Returns basic webpage on GET or POST. Added for request "manager/html"

Apache login

IP: 193.11.189.4
Port: 8081
Running: 2024/02/26 - 2024/03/03
Source : https://github.com/bocajspear1/honeyhttpd
Description:
Pretends to be a server with basic authentication.

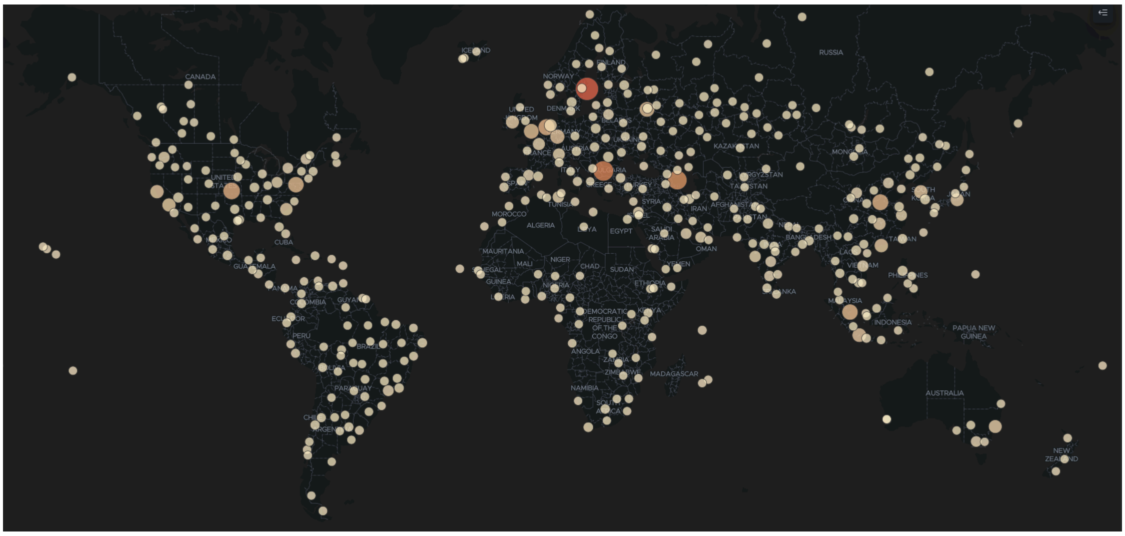
Outlook web login

IP: 193.11.189.4
Port: 8000
Running: 2024/02/13 - 2024/03/03
Source : https://github.com/joda32/owa-honeypot
Description:
Pretends to be an exposed outlook web server.

Metasploitable 2

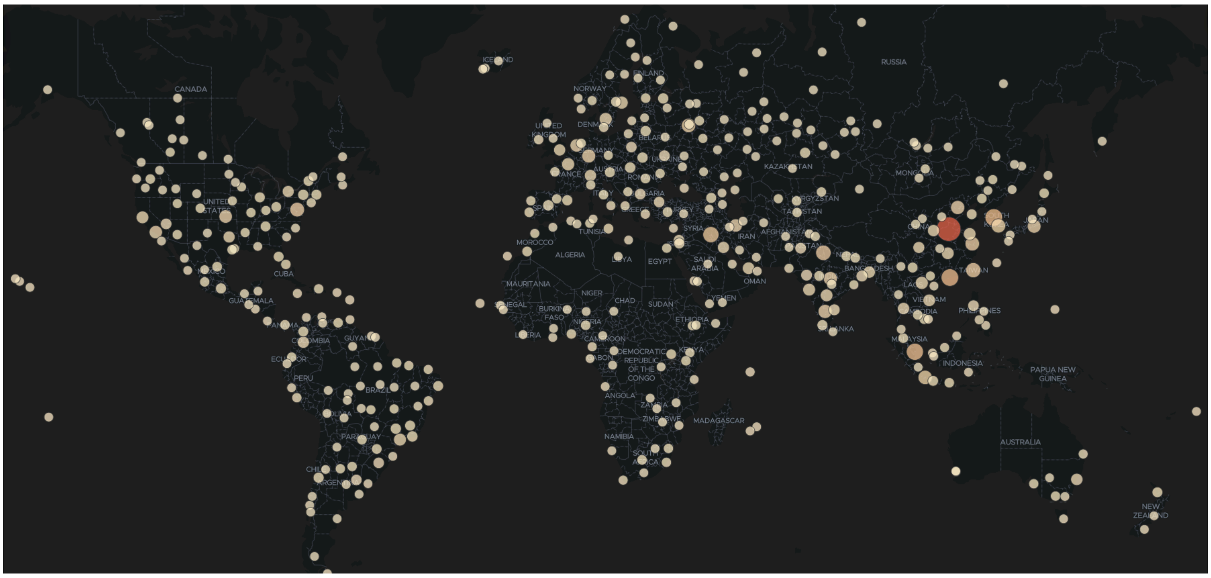
IP: 193.11.189.6
Source : https://docs.rapid7.com/metasploit/metasploitable-2/
Running: 2024/02/26 Only ran for 1 hour
Description:
A vm with several configured vulnerabilities.

Countries



(Image 1. Traffic amount from each country)

Because of local traffic and system logs Sweden has the most activity. But as seen in the picture our network has had a lot of activity. Then the most activity were from the USA, Europe and Asia. Apart from Sweden and based on the approximately 10,2 million total results in our Security Onion, Bulgaria, the Netherlands, England, Azerbaijan, China and Malaysia sent the most traffic to our system.



(Image 2. Traffic from unique IP-addresses)

The countries with the most unique IP-addresses were China, Iraq, Hong Kong, South Korea, Malaysia and India. So, mostly from Asia.

Attacks

During our two weeks of logging attacks against our system we faced a wide range of different attacks that aimed to attack and exploit different things in our system. We received a total of about 350 alerts on our system with high severity based on what we could find on the Security Onion Eval alerts window, this may seem like very little but we did however receive many tens of thousands of medium level severity alerts. The honeypots we used for this project mainly opened for vulnerabilities that were from the medium severity level which explains the lack of high severity alerts that we received. The attacks were mainly aimed towards the ports 8000, 8080 and 8081. These attacks mainly involved trying to bruteforce SSH, many command injection attempts, nmap scanning as well as many other more specific attacks that will be explained in further detail later on in the report. A timeline of all the attacks detected per day can be found at the end of the report.

As follows are some more attacks that occurred during the logging period that are interesting but could not be found in the alerts timeline via the Security Onion Eval alerts which is pasted in at the end of the report. Also included are the two most numerous medium severity alerts as well as the most common high severity alerts that we got during our information gathering period.

High Severity

3	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)
3	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)
71	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack
1	ET EXPLOIT Microsoft Exchange Pre-Auth Path Confusion M1 (CVE-2021-31207)
1	ET WORM TheMoon.linksys.router 1
21	ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35394)
2	ET EXPLOIT Xiongmai/HiSilicon DVR - Request for User Details - Possible CVE-2017-7577 Exploit Attempt

Most common medium severity alerts

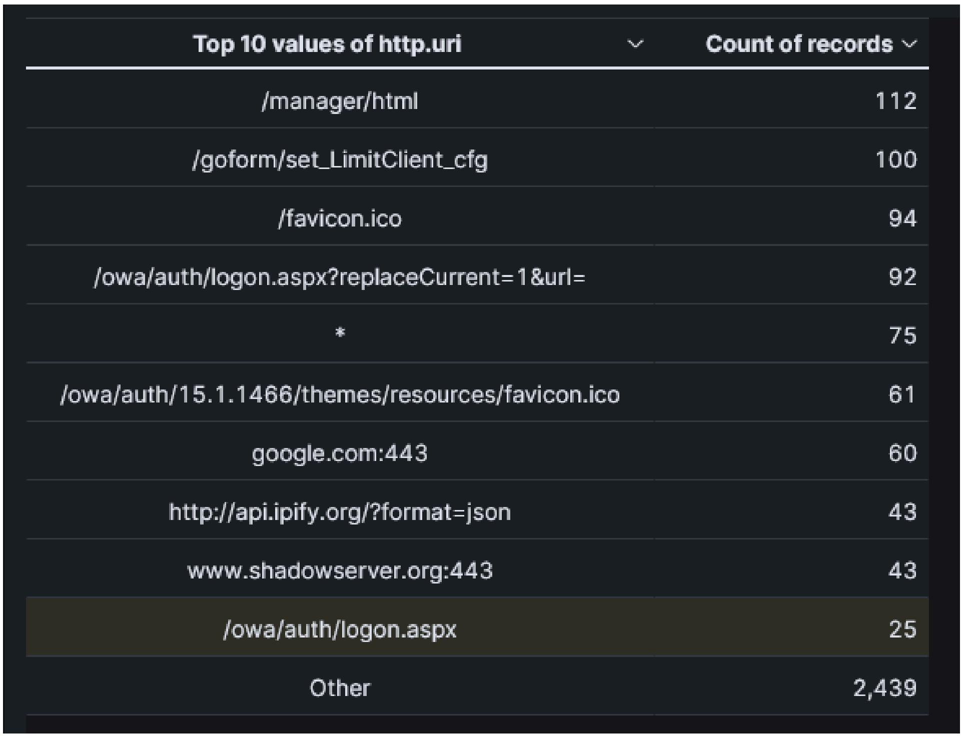
71 117	ET DROP Dshield Block Listed Source group 1
2 243	ET SCAN Suspicious inbound to MSSQL port 1433/ port 3306
2 680	ET DROP Spamhaus DROP Listed Traffic Inbound group 15

Most common high severity alerts

124	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
71	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack
53	ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

21 ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35394)
13 ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted

Common HTTP uri requests



Top 10 values of http.uri	Count of records
/manager/html	112
/goform/set_LimitClient_cfg	100
/favicon.ico	94
/owa/auth/logon.aspx?replaceCurrent=1&url=	92
*	75
/owa/auth/15.1.1466/themes/resources/favicon.ico	61
google.com:443	60
http://api.ipify.org/?format=json	43
www.shadowserver.org:443	43
/owa/auth/logon.aspx	25
Other	2,439

(Image 3. Some of the most common HTTP uri requests)

ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags) / (MSF style)
Probing to see if windows OS system lacks MS17-010 update which is the update that patched the eternalblue exploit. Eternalblue would exploit the Server Message Block (SMB) protocol to allow for remote execution of code, which was famously used in the WannaCry and NotPetya attacks. (CVE-2017-0144)

ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)
A critical command injection vulnerability discovered in March 2023 (CVSS 9.8) in LB-LINK wireless routers.
(Source: https://www.akamai.com/blog/security-research/cve-2023-26801-exploited-spreading-mirai-botnet)

ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
Nmap is a tool used for scanning networks to discover hosts and services on a computer network. This specific alert was triggered by “193.11.189.18” 124 times between 2024/02/19 - 2024/02/20, these scans were sent by another group in the lab.

ET WORM TheMoon.linksys.router 1
"TheMoon" is a worm that targets the Linksys routers. It was first identified in 2014 and exploits a vulnerability in certain models of Linksys routers which allows for unauthorized access.
(Source: https://www.computerworld.com/article/2487791/-the-moon--worm-infects-linksys-routers.html)

ET WEB_SERVER ThinkPHP RCE Exploitation Attempt
A remote code execution bug in the Chinese open source framework ThinkPHP, primarily targeting Internet of Things (IoT) devices.
(Source: https://www.tenable.com/blog/thinkphp-remote-code-execution-vulnerability-used-to-deploy-variety-of-malware-cve-2018-20062)

ET EXPLOIT Microsoft Exchange Pre-Auth Path Confusion M1 (CVE-2021-31207)
Microsoft Exchange Server authentication path pathing vulnerability.
(Source: https://www.cvedetails.com/cve/CVE-2021-31207)

Attack Summary

Over the course of our two week logging period our system encountered a large variety of different attacks aimed at exploiting different vulnerabilities. It was shocking to see the amount of different attack vectors that the attacks used even though our honeypots were pretty limited. Overall we can see in our findings how everyone is under constant attack from many different things. This shows the importance of knowing what is trying to attack or exploit your system so that you know how to mitigate these potential security risks in a proper way and to potentially stop larger attacks in the early stages by analyzing what kind of traffic your system is facing.

IoC

For our specific honeypots no specific IOCs would probably exist according to our gathered data. Instead of just normal IOCs such as unknown user or file creation, users logging in from unknown IPs could be generally applied as IOCs. Making sure all systems are up to date is a way to make sure vulnerabilities like eternalblue (MS17-010 update) won't be exploited.

We have gathered IOCs for the attacks for other devices that we found, this can be found at the end in the "IOCs for other vulnerabilities" section.

IDS Rules

To create rules to protect a network from these attacks several things can be done:

Using several available poor reputation ip lists, or other available rules to monitor the traffic.

Block all IPs taken from high severity or medium severity alerts.

Block POST /goform/set_LimitClient_cfg if a LB-LINK is in the network.

Summary

During our two weeks with this project we have learnt a lot about the current digital situation of the world. We have seen what kind of attacks and exploits potential attacks are using and where most of these attacks originate from. This has provided us with a comprehensive understanding and insights into the current state of digital security worldwide.
As seen above from our collected data most of the attacks recorded are just attackers sending out traffic to hopefully find a device that is exploitable and no specific targeted attacks. Another common example as seen in picture 3 is attackers trying default unsecured pages such as“/manager/html”.
Old exploits such as eternalblue are still being attempted which shows that it still works and people are not updating their systems which is a huge security risk.

To improve our methodology in the future and get more specific attacks, more specified honeypots that look more like vulnerable services should be used. Most of the attacks were not directed to us because of an attacker thinking we had a specific vulnerability but mostly because they send out massive amounts to try on all available IPs. More time with Metasploitable 2 is one example to hopefully receive more traffic specific for one of our systems.

Attack Timeline

High severity alerts

2024/03/01 02:48:41 PM - 2024/03/02 02:48:41 PM
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/29 02:48:41 PM - 2024/03/01 02:48:41 PM
ET SCAN Tomcat X-Y login credentials
ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/28 02:48:41 PM - 2024/02/29 02:48:41 PM
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)
ET POLICY External Oracle T3 Requests Inbound

2024/02/27 02:48:41 PM - 2024/02/28 02:48:41 PM
ET EXPLOIT HackingTrio UA (Hello, World)
ET SCAN Mirai Variant User-Agent (Inbound)
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/26 02:48:41 PM - 2024/02/27 02:48:41 PM
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)
ET POLICY External Oracle T3 Requests Inbound

2024/02/25 02:48:41 PM - 2024/02/26 02:48:41 PM
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/24 02:48:41 PM - 2024/02/25 02:48:41 PM
ET WEB_SERVER ThinkPHP RCE Exploitation Attempt

2024/02/23 02:48:41 PM - 2024/02/24 02:48:41 PM
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/22 02:48:41 PM - 2024/02/23 02:48:41 PM
ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound (CVE-2023-1389)

2024/02/21 02:48:41 PM - 2024/02/22 02:48:41 PM
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/20 02:48:41 PM - 2024/02/21 02:48:41 PM
ET POLICY External Oracle T3 Requests Inbound
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/19 02:48:41 PM - 2024/02/20 02:48:41 PM
ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
ET EXPLOIT HackingTrio UA (Hello, World)
ET SCAN Mirai Variant User-Agent (Inbound)

2024/02/18 02:48:41 PM - 2024/02/19 02:48:41 PM
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/17 02:48:41 PM - 2024/02/18 02:48:41 PM
ET EXPLOIT D-Link Devices Home Network Administration Protocol Command Execution
ET WEB_SERVER Possible D-Link Router HNAP Protocol Security Bypass Attempt
ET WEB_SERVER WGET Command Specifying Output in HTTP Headers
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)
ET EXPLOIT Possible Zimbra Autodiscover Servlet XXE (CVE-2019-9670)
ET EXPLOIT Zimbra <8.8.11 - XML External Entity Injection/SSRF Attempt (CVE-2019-9621)
ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.
ET HUNTING Suspicious Chmod Usage in URI (Inbound)

2024/02/16 02:48:41 PM - 2024/02/17 02:48:41 PM
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/15 02:48:41 PM - 2024/02/16 02:48:41 PM
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/14 02:48:41 PM - 2024/02/15 02:48:41 PM
ET SCAN Tomcat Auth Brute Force attempt (admin)
ET SCAN Tomcat admin-admin login credentials
ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted
ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)

2024/02/13 02:48:41 PM - 2024/02/14 02:48:41 PM
ET EXPLOIT Generic ADSL Router DNS Change GET Request
ET EXPLOIT Generic ADSL Router DNS Change Request
ET EXPLOIT Possible dlink-DSL2640B DNS Change Attempt
ET EXPLOIT TP-LINK DNS Change GET Request (DNSChanger EK)
ET EXPLOIT TP-LINK TL-WR340G Router DNS Change GET Request
ET EXPLOIT TP-LINK TL-WR841N Router DNS Change GET Request
ET SCAN Tomcat Auth Brute Force attempt (admin)
ET SCAN Tomcat admin-admin login credentials

IOCs for other vulnerabilities

(CVE-2023-26801)

85.208.139.67
45.66.230.32
103.95.196.149
193.42.32.40

446bf64f576f3ee1e3fa130005e6cea27ec4acfd8af7dd067d39367159ebee62: ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped

eb143186410a79e876cb2e4a09eadba530e7b7ffb893dccf6b6e9a5febfabb46: ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped

048e4e09396cd9e6c1bb2ac89fdb243d7669929499850940bb0a2737aaf0fb4d: ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped ac4750995b6159238f8b61ea31a5de45c2414cc37d46b360ac3746ec7188bfe5: ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, with debug_info, not stripped

9507e3fd6a74289998c5460060038d45271f175a0485db63379f494843b1f7f6: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

feca0b6fd6bec792c79d3a4dcf4e43aea9e5ff978d5b688e0a77b593144ac569: ELF 32-bit LSB executable, ARM, version 1 (ARM), dynamically linked, interpreter /lib/ld-uClibc.so.0, stripped

40f8be79003d9fe2ac0e0f6890958c731bf5869e0f52c869c061e88a80cc09a2: ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, stripped