

Usman Ahmad

Danyal Bhatti

Alberto Munar

Professor Asma Paracha

SRT411 Digital Data Analysis

March 30th, 2022

Phase 2: Log Collection

Introduction

We have multiple goals for this phase of the project. They include identifying the logs we need to collect from our system built in phase 1. Create users and generate data from them that would be considered normal and malicious. Create logs from the generated traffic and analyze them.

Objective

To achieve our goals within this phase we will run scans and collect the data. We will use Logstash for the collection process. We will create traffic by pinging all the machines and scanning their ports to see what services are running. We will also scan the console looking for files and folders in each machine. We create and run queries using SQLmap on our MySQL server. Lastly, we will show normal traffic such as web browsing and ssh connection as well as malicious traffic through attacks.

Contents

Introduction.....	1
Objective.....	1
Information Gathering:	3
NMAP Scans:.....	3
Greenbone Scanning:	8
Pings.....	15
Snort:.....	16
Snort Configuration:	16
Snort Rules:.....	17
Attacks:	18
DDoS or DoS attack:	19
Snort event Logging for DoS attack:	20
SSH Logins and Brute Force Attacks:	21
Snort Logs and events triggered by SSH Brute force	21
SSH Connection:.....	22
Snort Pick up of ssh connection:.....	23
Deep Scan of M1 of each port service and details:.....	24
Snort collection of data:	24
Security Goals, Vulnerabilities and Threats	25
How Data Collection help you achieve your goal:	25
Explain Data Collection:.....	25
Data Collection:	26
Brute Force Attack:.....	26
DDoS Attack:.....	27
Nmap Scan:.....	28
Greenbone Scan Results:	29
Snort Files/Logs collected and sent to Kali	30
References.....	31

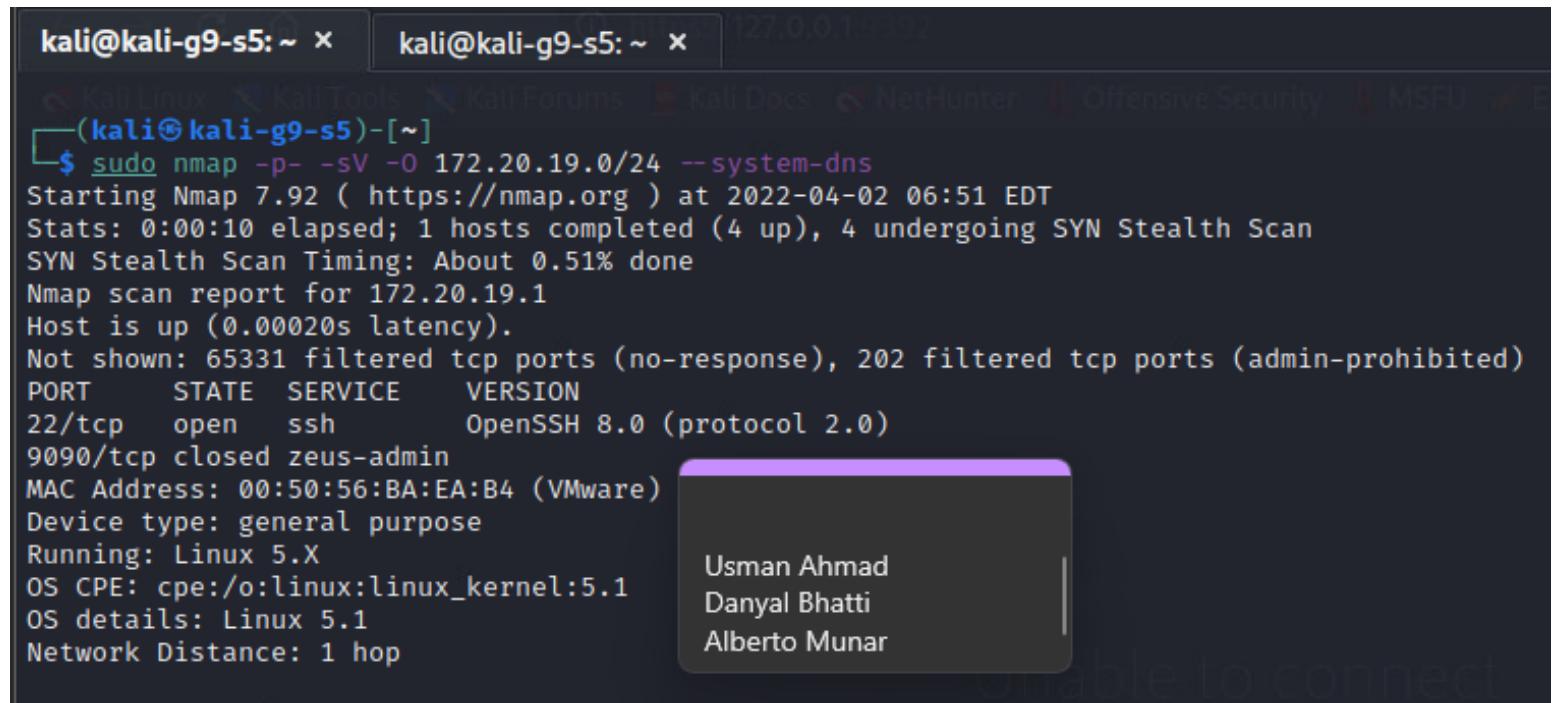
Information Gathering:

NMAP Scans:

```
Nmap -p- -sV -O 172.20.19.0/24 --system-dns
```

172.20.19.1 M1

172.20.21.1 Attack Network



```
kali@kali-g9-s5: ~ x kali@kali-g9-s5: ~ x [27.0.0.1:592]
└─(kali㉿kali-g9-s5)-[~]
$ sudo nmap -p- -sV -O 172.20.19.0/24 --system-dns
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-02 06:51 EDT
Stats: 0:00:10 elapsed; 1 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.51% done
Nmap scan report for 172.20.19.1
Host is up (0.00020s latency).
Not shown: 65331 filtered tcp ports (no-response), 202 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0 (protocol 2.0)
9090/tcp  closed zeus-admin
MAC Address: 00:50:56:BA:EA:B4 (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.1
OS details: Linux 5.1
Network Distance: 1 hop
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

All the Open Ports:

```
Nmap scan report for 172.20.19.2
Host is up (0.00014s latency).
Not shown: 65487 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp     open  ftp              Microsoft ftfd
22/tcp     open  ssh              OpenSSH 7.1 (protocol 2.0)
80/tcp     open  http             Microsoft IIS httpd 7.5
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1617/tcp   open  java-rmi        Java RMI
3000/tcp   open  http             WEBrick httpd 1.3.1 (Ruby 2.3.1 (2016-04-26))
3306/tcp   open  mysql            MySQL 5.5.20-log
3389/tcp   open  ssl/ms-wbt-server?
3700/tcp   open  giop             CORBA naming service
3820/tcp   open  ssl/giop         CORBA naming service
3920/tcp   open  ssl/exasoftport1? Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
4848/tcp   open  ssl/http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp   open  java-message-service Java Message Service 301
8009/tcp   open  ajp13            Apache Jserv (Protocol v1.3)
8019/tcp   open  qbdb?            Apache Tomcat/Coyote JSP engine 1.1
8022/tcp   open  http             PostgreSQL DB
8028/tcp   open  postgresql       ManageEngine Desktop Central DesktopCentralServer
8031/tcp   open  ssl/unknown      Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8032/tcp   open  desktop-central  Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8080/tcp   open  http             Apache Tomcat/Coyote JSP engine 1.1 you are unable to load a
8181/tcp   open  ssl/http         Apache Tomcat/Coyote JSP engine 1.1 you are unable to load a
8282/tcp   open  http             Apache Tomcat/Coyote JSP engine 1.1 you are unable to load a
8443/tcp   open  ssl/https-alt?  ManageEngine Desktop Central DesktopCentralServer or network
8444/tcp   open  desktop-central  Jetty winstone-2.8
8484/tcp   open  http             Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
8585/tcp   open  http             Java RMI
8686/tcp   open  java-rmi        Microsoft Windows RPC
9200/tcp   open  wap-wsp?        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9300/tcp   open  vrace?          Microsoft Windows RPC
47001/tcp  open  http             Microsoft Windows RPC
49152/tcp  open  msrpc            Microsoft Windows RPC
49153/tcp  open  msrpc            Microsoft Windows RPC
49154/tcp  open  msrpc            Microsoft Windows RPC
49155/tcp  open  msrpc            Microsoft Windows RPC
49176/tcp  open  unknown          Microsoft Windows RPC
49200/tcp  open  msrpc            Microsoft Windows RPC
49201/tcp  open  java-rmi        Java RMI
49203/tcp  open  msrpc            Microsoft Windows RPC
49204/tcp  open  tcpwrapped       Apache Mina sshd 0.8.0 (protocol 2.0)
49264/tcp  open  ssh              Jenkins TcpSlaveAgentListener
49265/tcp  open  jenkins-listener Jenkins TcpSlaveAgentListener
63517/tcp  open  java-rmi        Java RMI
63520/tcp  open  unknown          Microsoft Windows RPC
63521/tcp  open  unknown          Microsoft Windows RPC
63522/tcp  open  unknown          Microsoft Windows RPC
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

The following is the OS information and other details about the service types and the TCP fingerprint:

172.20.19.3 M3:

172.20.21.3 Attack Network

```
Nmap scan report for 172.20.19.3
Host is up (0.00020s latency).
Not shown: 65329 filtered tcp ports (no-response), 202 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.37 ((centos))
443/tcp   closed https
9090/tcp closed zeus-admin
MAC Address: 00:50:56:BA:6F (VMware)
Device type: general purpose|storage-misc|WAP
Running (JUST GUESSING): Linux 5.X|3.X|4.X|2.6.X (98%), HP embedded (91%), Ubiquiti embedded (89%), Ubiquiti AirOS 5.X (89%)
OS CPE: cpe:/o:linux:linux_kernel:5.1 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6 cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:ubnt:airmax_nanostation cpe:/o:ubnt:airos:5.2.6
Aggressive OS guesses: Linux 5.1 (98%), Linux 3.10 - 4.11 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.13 (95%), Linux 5.4 (94%), Linux 3.16 - 4.6 (93%), Linux 2.6.22 - 2.6.36 (93%), Linux 5.0 - 5.4 (93%), Linu
x 2.6.39 (93%), Linux 4.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

172.20.19.4 M4:

172.20.21.4 Attack Network

```
Nmap scan report for 172.20.19.4
Host is up (0.00017s latency).
Not shown: 65330 filtered tcp ports (no-response), 202 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.37 ((centos))
9090/tcp closed zeus-admin
MAC Address: 00:50:56:BA:74:42 (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.1
OS details: Linux 5.1
Network Distance: 1 hop
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

172.20.19.5 M5:

```
Nmap scan report for 172.20.19.5 (kali)
Host is up (0.00014s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5985/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp  open  msrpc        Microsoft Windows RPC
49665/tcp  open  msrpc        Microsoft Windows RPC
49666/tcp  open  msrpc        Microsoft Windows RPC
49667/tcp  open  msrpc        Microsoft Windows RPC
49668/tcp  open  msrpc        Microsoft Windows RPC
49669/tcp  open  msrpc        Microsoft Windows RPC
49670/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 00:50:56:BA:E5:66 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

ORACLE TO CONNECT

```
TCP/IP fingerprint:
```

```
OS:SCAN(V=7.92%E=4%D=4/2%OT=135%CT=1%CU=31928%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=62482D10%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=111%TI=I%CI=I%II=I%
OS:SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5
OS:B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
OS:ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+%
OS:F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=
OS:80%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=80%CD=Z)
```

```
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Greenbone Scanning:

The Screenshots below show the Vulnerabilities found over the systems on the network. These scans were performed on the Attack Network Interface. There were three Hosts detected.

The screenshot shows the Greenbone Security Assistant interface running in a VMware Workstation window. The main view displays a table of vulnerabilities found across three hosts. The columns include:

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)	10.0 (High)	95 %	172.20.21.1		80/tcp	Sat, Apr 2, 2022 3:13 PM UTC
Oracle MySQL 'my.conf' Security Bypass Vulnerability (Windows)	10.0 (High)	80 %	172.20.21.1		3306/tcp	Sat, Apr 2, 2022 3:01 PM UTC
Oracle MySQL Security Updates (oct2016-2881722) 09 - Windows	10.0 (High)	80 %	172.20.21.1		3306/tcp	Sat, Apr 2, 2022 3:01 PM UTC
Elasticsearch End of Life Detection	10.0 (High)	80 %	172.20.21.1		9200/tcp	Sat, Apr 2, 2022 3:05 PM UTC
Apache Tomcat End Of Life Detection (Windows)	10.0 (High)	80 %	172.20.21.1		8282/tcp	Sat, Apr 2, 2022 3:07 PM UTC
Apache Axis2 axis2-admin default credentials	10.0 (High)	98 %	172.20.21.1		8282/tcp	Sat, Apr 2, 2022 3:07 PM UTC
Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)	10.0 (High)	99 %	172.20.21.1		3389/tcp	Sat, Apr 2, 2022 3:13 PM UTC
ManageEngine Desktop Central 9 FileUploadServlet connectionId Vulnerability	10.0 (High)	99 %	172.20.21.1		8022/tcp	Sat, Apr 2, 2022 3:11 PM UTC
ManageEngine Desktop Central Remote Control Privilege Violation Vulnerability	10.0 (High)	80 %	172.20.21.1		8022/tcp	Sat, Apr 2, 2022 3:05 PM UTC
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.0 (High)	95 %	172.20.21.1		445/tcp	Sat, Apr 2, 2022 3:13 PM UTC
MySQL / MariaDB weak password	9.0 (High)	95 %	172.20.21.1		3306/tcp	Sat, Apr 2, 2022 3:07 PM UTC
Apache Tomcat 'MultipartStream' Class Denial of Service Vulnerability (Windows)	7.8 (High)	80 %	172.20.21.1		8282/tcp	Sat, Apr 2, 2022 3:07 PM UTC
OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows)	7.8 (High)	80 %	172.20.21.1		22/tcp	Sat, Apr 2, 2022 3:01 PM UTC
Oracle MySQL < 8.0.22 Security Update (cpuoc2020) - Windows	7.7 (High)	80 %	172.20.21.1		3306/tcp	Sat, Apr 2, 2022 3:01 PM UTC
OpenSSH X11 Forwarding Security Bypass Vulnerability (Windows)	7.5 (High)	80 %	172.20.21.1		22/tcp	Sat, Apr 2, 2022 3:01 PM UTC
Oracle MySQL Multiple Unspecified vulnerabilities-02 Oct14 (Windows)	7.5 (High)	80 %	172.20.21.1		3306/tcp	Sat, Apr 2, 2022 3:01 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	7.5 (High)	99 %	172.20.21.1		8009/tcp	Sat, Apr 2, 2022 3:08 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	7.5 (High)	99 %	172.20.21.1		8019/tcp	Sat, Apr 2, 2022 3:08 PM UTC
phpinfo() output Reporting	7.5 (High)	80 %	172.20.21.2		80/tcp	Sat, Apr 2, 2022 2:55 PM UTC
Oracle MySQL Security Updates (jan2018-3236628) 04 - Windows	7.5 (High)	80 %	172.20.21.1		3306/tcp	Sat, Apr 2, 2022 3:01 PM UTC
Oracle MySQL < 5.7.32 Security Update (cpuoc2020) - Windows	7.5 (High)	80 %	172.20.21.1		3306/tcp	Sat, Apr 2, 2022 3:01 PM UTC

The interface also includes a navigation bar with tabs like Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, Help, and a user menu. The bottom status bar shows system information and the date: Sat, Apr 2, 2022 3:01 PM UTC.

Screenshot of a VMware Workstation window showing multiple VMs running. The active VM is "SRT41INAA_2221_G09_M5 - VMware Workstation". The browser window displays the "Greenbone Security Assistant" interface at https://127.0.0.1:9392/report/5054f51f-ac0d-4fd1-88ff-e50dda604357. The interface shows a list of vulnerabilities across various hosts, including Apache Tomcat, Oracle MySQL, and SSL/TLS issues. A user profile for "Usman Ahmad" is visible in the top right corner.

The following Hosts were

Screenshot of the "Greenbone Security Assistant" interface showing a report for "Report: Sat, Apr 2, 2022 2:51 PM UTC". The report details findings across 3 hosts (18 of 29), 15 applications (2 of 3), 103 operating systems, 16 closed CVEs, 4 TLS certificates, 0 error messages, and 0 user tags. The table lists IP addresses, hostnames, OS, ports, apps, distance, auth, start, end, and severity. A user profile for "Usman Ahmad" is visible in the top right corner.

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity
172.20.21.1		Ubuntu	18	23			Sat, Apr 2, 2022 2:52 PM UTC	Sat, Apr 2, 2022 3:13 PM UTC	35	86	7	0	0	128	10.0 (High)
172.20.21.2		Ubuntu	2	3			Sat, Apr 2, 2022 2:52 PM UTC	Sat, Apr 2, 2022 3:06 PM UTC	1	2	1	0	0	4	7.5 (High)
172.20.21.3		Ubuntu	2	3			Sat, Apr 2, 2022 2:52 PM UTC	Sat, Apr 2, 2022 3:05 PM UTC	0	2	1	0	0	3	5.8 (Medium)

The Ports found from The Greenbone Scan:

SRT41NAA_2221_G09_M5 – VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

Warning: Potential Security Risk

Greenbone Security Assistant

https://127.0.0.1:9392/report/5054f51f-ac0d-4fd1-88ff-e50dda604357

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Greenbone Security Assistant

Report: Sat, Apr 2, 2022 2:51 PM UTC

ID: 5054f51f-ac0d-4fd1-88ff-e50dda604357 Created: Sat, Apr 2, 2022 2:52 PM UTC Modified: Sat, Apr 2, 2022 3:13 PM UTC Owner: admin

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags

Ports (18 of 29)

Hosts (3 of 4)

Severity ▼

Port	Hosts	Severity
80/tcp	3	10.0 (High)
3306/tcp	1	10.0 (High)
3389/tcp	1	10.0 (High)
8022/tcp	1	10.0 (High)
8282/tcp	1	10.0 (High)
9200/tcp	1	10.0 (High)
445/tcp	1	9.3 (High)
22/tcp	3	7.8 (High)
21/tcp	1	7.5 (High)
1617/tcp	1	7.5 (High)
8009/tcp	1	7.5 (High)
8019/tcp	1	7.5 (High)
8443/tcp	1	5.4 (Medium)
135/tcp	1	5.0 (Medium)
3820/tcp	1	5.0 (Medium)
4848/tcp	1	5.0 (Medium)
8181/tcp	1	5.0 (Medium)
3920/tcp	1	4.0 (Medium)

(Applied filter: apply_overrides=0 levels=html rows=100 min_qod=70 first=1 sort=reverse=severity)

To direct input to this VM, click inside or press Ctrl+G.

0°C Cloudy

10:17 PM 2022-04-02

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Applications:

The screenshot shows the Greenbone Security Assistant interface. At the top, there's a navigation bar with links like Kali Linux, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. Below the navigation is a main menu with sections: Dashboards, Scans, Assets, Resilience, SecInfo (selected), Configuration, Administration, and Help.

The main content area is titled "Report: Sat, Apr 2, 2022 2:51 PM UTC" and shows various statistics: ID: 5054f51f-ac0d-4fd1-88ff-e50dda604357, Created: Sat, Apr 2, 2022 2:52 PM UTC, Modified: Sat, Apr 2, 2022 3:13 PM UTC, Owner: admin.

A modal window is open, listing users: Usman Ahmad, Danyal Bhatti, Alberto Munar. The modal has a "Done" button at the top right.

The "Applications" section is selected in the navigation bar. It displays a table of CPE entries with columns: Hosts, Occurrences, and Severity. The table shows 15 entries, with the first few being:

CPE	Hosts	Occurrences	Severity
cpe:/a:oracle:mysql:5.5.20	1	2	10.0 (High)
cpe:/a:microsoft:internet_information_services:7.5	1	2	10.0 (High)
cpe:/a:openbsd:openssh:7.1	1	2	7.8 (High)
cpe:/a:elasticsearch:logstash:1.1.1	1	2	N/A
cpe:/a:apache:axis2:1.6.0	1	2	N/A
cpe:/a:microsoft:ftp_service	1	1	N/A
cpe:/a:ruby-lang:ruby:2.3.1	1	2	N/A
cpe:/a:oracle:glassfish_server:4.0	1	2	N/A
cpe:/a:elasticsearch:elasticsearch:1.1.1	1	2	N/A
cpe:/a:ruby-lang:webrick:1.3.1	1	2	N/A
cpe:/a:zohocorp:management_desktop_central:91084	1	2	N/A
cpe:/a:apache:tomcat:8.0.33	1	2	N/A
cpe:/a:apache:http_server:2.4.37	2	2	N/A
cpe:/a:php:php:7.2.24	2	2	N/A
cpe:/a:openbsd:openssh:8.0	2	2	N/A

(Applied filter: apply_overrides=0 levels=html rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Operating Systems:

Report: Sat, Apr 2, 2022 2:51 PM UTC

Operating System	CPE	Hosts	Severity
Microsoft Windows	cpe:/o:microsoft:windows	1	10.0 (High)
CentOS	cpe:/o:centos:centos	2	7.5 (High)

User Activity:

- Usman Ahmad
- Danyal Bhatti
- Alberto Munar

CVEs:

CVE	NVT	Hosts	Occurrences	Severity
CVE-2015-1635	MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)	1	1	10.0 (High)
CVE-2016-6662	Oracle MySQL myc.com Security Bypass Vulnerability (Windows)	1	1	10.0 (High)
CVE-2016-5584 CVE-2016-6662 CVE-2016-7440	Oracle MySQL Security Updates (oct2016-2881722) 09 - Windows	1	1	10.0 (High)
CVE-2010-0219	Apache Axis2 axis2-admin default credentials	1	1	10.0 (High)
CVE-2019-0708	Microsoft Windows Remote Desktop Service 'CVE-2019-0708' Remote Code Execution	1	1	10.0 (High)
CVE-2015-8249	ManageEngine Desktop Central 9 FileUploadServlet connectionId Vulnerability	1	1	10.0 (High)
CVE-2017-7213	ManageEngine Desktop Central Remote Control Privilege Violation Vulnerability	1	1	10.0 (High)
CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	1	1	9.3 (High)
CVE-2016-3092	Apache Tomcat 'MultipartStream' Class Denial of Service Vulnerability (Windows)	1	1	7.8 (High)
CVE-2016-6515 CVE-2016-6210	OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows)	1	1	7.8 (High)
CVE-2020-14878 CVE-2020-14828 CVE-2020-14830 CVE-2020-14836 CVE-2020-14846 CVE-2020-14800 CVE-2020-14821				
CVE-2020-14829 CVE-2020-14848 CVE-2020-14852 CVE-2020-14814 CVE-2020-14804 CVE-2020-14773 CVE-2020-14777				
CVE-2020-14785 CVE-2020-14794 CVE-2020-14809 CVE-2020-14837 CVE-2020-14839 CVE-2020-14845 CVE-2020-14861				
CVE-2020-14866 CVE-2020-14868 CVE-2020-14888 CVE-2020-14891 CVE-2020-14893 CVE-2020-14786 CVE-2020-14844				
CVE-2020-14870 CVE-2020-14873 CVE-2020-14838 CVE-2020-14860 CVE-2020-14791				
CVE-2016-1908	OpenSSH X11 Forwarding Security Bypass Vulnerability (Windows)	1	1	7.5 (High)
CVE-2014-6559 CVE-2014-6555 CVE-2014-6507 CVE-2014-6500 CVE-2014-6496 CVE-2014-6494 CVE-2014-6491 CVE-2014-6469	Oracle MySQL Multiple Unspecified vulnerabilities-02 Oct14 (Windows)	1	1	7.5 (High)
CVE-2014-6464				
CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	1	2	7.5 (High)
CVE-2015-0411 CVE-2014-6568 CVE-2015-0382 CVE-2015-0381 CVE-2015-0374	Oracle MySQL Multiple Unspecified vulnerabilities-01 Feb15 (Windows)	1	1	7.5 (High)

Closed CVE's:

Greenbone Security Assistant

Report: Sat, Apr 2, 2022 2:51 PM UTC Done

ID: 5054f51f-ac0d-4fd1-88ff-e50dda604357 Created: Sat, Apr 2, 2022 2:52 PM UTC Modified: Sat, Apr 2, 2022 3:13 PM UTC Owner: admin

Information	Results (135 of 387)	Hosts (3 of 4)	Ports (18 of 29)	Applications (15 of 15)	Operating Systems (2 of 3)	CVEs (103 of 103)	Closed CVEs (16 of 16)	TLS Certificates (4 of 4)	Error Messages (0 of 0)	User Tags (0)																																																																				
<table border="1"> <thead> <tr> <th>CVE</th> <th>Host</th> <th>NVT</th> <th>Severity ▼</th> </tr> </thead> <tbody> <tr><td>CVE-2010-0020</td><td>172.20.21.1</td><td>Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)</td><td>10.0 (High)</td></tr> <tr><td>CVE-2010-0021</td><td>172.20.21.1</td><td>Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)</td><td>10.0 (High)</td></tr> <tr><td>CVE-2010-0022</td><td>172.20.21.1</td><td>Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)</td><td>10.0 (High)</td></tr> <tr><td>CVE-2010-0231</td><td>172.20.21.1</td><td>Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)</td><td>10.0 (High)</td></tr> <tr><td>CVE-2009-2526</td><td>172.20.21.1</td><td>Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability</td><td>10.0 (High)</td></tr> <tr><td>CVE-2009-2532</td><td>172.20.21.1</td><td>Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability</td><td>10.0 (High)</td></tr> <tr><td>CVE-2009-3103</td><td>172.20.21.1</td><td>Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability</td><td>10.0 (High)</td></tr> <tr><td>CVE-2006-3439</td><td>172.20.21.1</td><td>Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)</td><td>10.0 (High)</td></tr> <tr><td>CVE-2000-0884</td><td>172.20.21.1</td><td>Microsoft M500-078 security check</td><td>7.5 (High)</td></tr> <tr><td>CVE-2003-0822</td><td>172.20.21.1</td><td>Microsoft M503-051 security check</td><td>7.5 (High)</td></tr> <tr><td>CVE-2003-0824</td><td>172.20.21.1</td><td>Microsoft M503-051 security check</td><td>7.5 (High)</td></tr> <tr><td>CVE-2000-0746</td><td>172.20.21.1</td><td>Microsoft M500-060 security check</td><td>7.5 (High)</td></tr> <tr><td>CVE-2000-1104</td><td>172.20.21.1</td><td>Microsoft M500-060 security check</td><td>7.5 (High)</td></tr> <tr><td>CVE-2004-0204</td><td>172.20.21.1</td><td>Microsoft M504-017 security check</td><td>7.5 (High)</td></tr> <tr><td>CVE-2000-0778</td><td>172.20.21.1</td><td>Microsoft M500-058 security check</td><td>5.0 (Medium)</td></tr> <tr><td>CVE-2000-0097</td><td>172.20.21.1</td><td>Microsoft M500-06 security check</td><td>5.0 (Medium)</td></tr> </tbody> </table>											CVE	Host	NVT	Severity ▼	CVE-2010-0020	172.20.21.1	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	CVE-2010-0021	172.20.21.1	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	CVE-2010-0022	172.20.21.1	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	CVE-2010-0231	172.20.21.1	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	CVE-2009-2526	172.20.21.1	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (High)	CVE-2009-2532	172.20.21.1	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (High)	CVE-2009-3103	172.20.21.1	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (High)	CVE-2006-3439	172.20.21.1	Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)	10.0 (High)	CVE-2000-0884	172.20.21.1	Microsoft M500-078 security check	7.5 (High)	CVE-2003-0822	172.20.21.1	Microsoft M503-051 security check	7.5 (High)	CVE-2003-0824	172.20.21.1	Microsoft M503-051 security check	7.5 (High)	CVE-2000-0746	172.20.21.1	Microsoft M500-060 security check	7.5 (High)	CVE-2000-1104	172.20.21.1	Microsoft M500-060 security check	7.5 (High)	CVE-2004-0204	172.20.21.1	Microsoft M504-017 security check	7.5 (High)	CVE-2000-0778	172.20.21.1	Microsoft M500-058 security check	5.0 (Medium)	CVE-2000-0097	172.20.21.1	Microsoft M500-06 security check	5.0 (Medium)
CVE	Host	NVT	Severity ▼																																																																											
CVE-2010-0020	172.20.21.1	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)																																																																											
CVE-2010-0021	172.20.21.1	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)																																																																											
CVE-2010-0022	172.20.21.1	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)																																																																											
CVE-2010-0231	172.20.21.1	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)																																																																											
CVE-2009-2526	172.20.21.1	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (High)																																																																											
CVE-2009-2532	172.20.21.1	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (High)																																																																											
CVE-2009-3103	172.20.21.1	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (High)																																																																											
CVE-2006-3439	172.20.21.1	Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)	10.0 (High)																																																																											
CVE-2000-0884	172.20.21.1	Microsoft M500-078 security check	7.5 (High)																																																																											
CVE-2003-0822	172.20.21.1	Microsoft M503-051 security check	7.5 (High)																																																																											
CVE-2003-0824	172.20.21.1	Microsoft M503-051 security check	7.5 (High)																																																																											
CVE-2000-0746	172.20.21.1	Microsoft M500-060 security check	7.5 (High)																																																																											
CVE-2000-1104	172.20.21.1	Microsoft M500-060 security check	7.5 (High)																																																																											
CVE-2004-0204	172.20.21.1	Microsoft M504-017 security check	7.5 (High)																																																																											
CVE-2000-0778	172.20.21.1	Microsoft M500-058 security check	5.0 (Medium)																																																																											
CVE-2000-0097	172.20.21.1	Microsoft M500-06 security check	5.0 (Medium)																																																																											

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

TLS Certificates:

Greenbone Security Assistant

Report: Sat, Apr 2, 2022 2:51 PM UTC Done

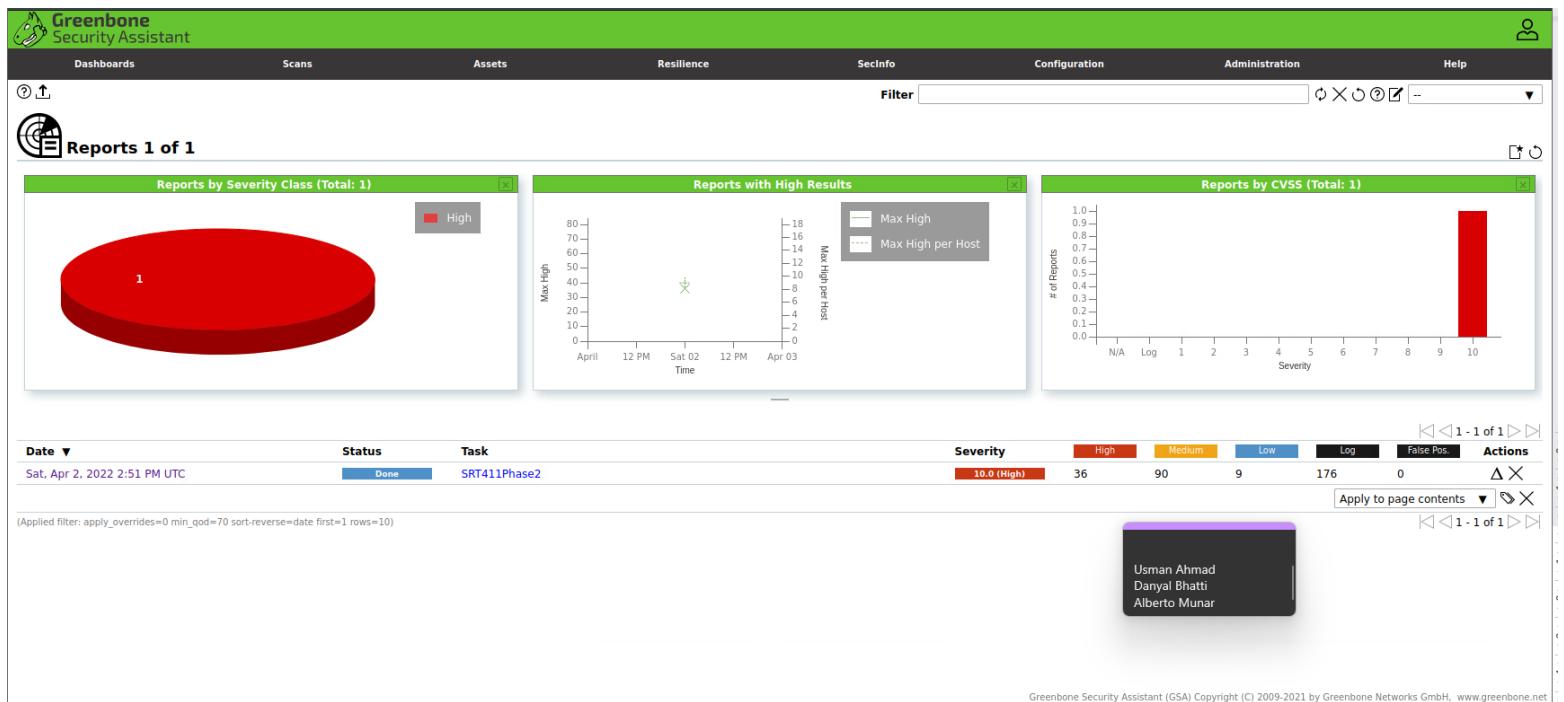
ID: 5054f51f-ac0d-4fd1-88ff-e50dda604357 Created: Sat, Apr 2, 2022 2:52 PM UTC Modified: Sat, Apr 2, 2022 3:13 PM UTC Owner: admin

Information	Results (135 of 387)	Hosts (3 of 4)	Ports (18 of 29)	Applications (15 of 15)	Operating Systems (2 of 3)	CVEs (103 of 103)	Closed CVEs (16 of 16)	TLS Certificates (4 of 4)	Error Messages (0 of 0)	User Tags (0)																																								
<table border="1"> <thead> <tr> <th>Issuer DN ▲</th> <th>Serial</th> <th>Activates</th> <th>Expires</th> <th>IP</th> <th>Hostname</th> <th>Port</th> <th>Actions</th> </tr> </thead> <tbody> <tr><td>CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US</td><td>04A9972F</td><td>Wed, May 15, 2013 9:33 AM UTC</td><td>Sat, May 13, 2023 9:33 AM UTC</td><td>172.20.21.1</td><td></td><td>8181</td><td></td></tr> <tr><td>CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US</td><td>04A9972F</td><td>Wed, May 15, 2013 9:33 AM UTC</td><td>Sat, May 13, 2023 9:33 AM UTC</td><td>172.20.21.1</td><td></td><td>3820</td><td></td></tr> <tr><td>CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US</td><td>04A9972F</td><td>Wed, May 15, 2013 9:33 AM UTC</td><td>Sat, May 13, 2023 9:33 AM UTC</td><td>172.20.21.1</td><td></td><td>4848</td><td></td></tr> <tr><td>CN=wmeta3</td><td>56A7E2781A0CFE884B83AF533EB014D1</td><td>Fri, Nov 19, 2021 1:37 AM UTC</td><td>Sat, May 21, 2022 12:37 AM UTC</td><td>172.20.21.1</td><td></td><td>3389</td><td></td></tr> </tbody> </table>											Issuer DN ▲	Serial	Activates	Expires	IP	Hostname	Port	Actions	CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US	04A9972F	Wed, May 15, 2013 9:33 AM UTC	Sat, May 13, 2023 9:33 AM UTC	172.20.21.1		8181		CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US	04A9972F	Wed, May 15, 2013 9:33 AM UTC	Sat, May 13, 2023 9:33 AM UTC	172.20.21.1		3820		CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US	04A9972F	Wed, May 15, 2013 9:33 AM UTC	Sat, May 13, 2023 9:33 AM UTC	172.20.21.1		4848		CN=wmeta3	56A7E2781A0CFE884B83AF533EB014D1	Fri, Nov 19, 2021 1:37 AM UTC	Sat, May 21, 2022 12:37 AM UTC	172.20.21.1		3389	
Issuer DN ▲	Serial	Activates	Expires	IP	Hostname	Port	Actions																																											
CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US	04A9972F	Wed, May 15, 2013 9:33 AM UTC	Sat, May 13, 2023 9:33 AM UTC	172.20.21.1		8181																																												
CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US	04A9972F	Wed, May 15, 2013 9:33 AM UTC	Sat, May 13, 2023 9:33 AM UTC	172.20.21.1		3820																																												
CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US	04A9972F	Wed, May 15, 2013 9:33 AM UTC	Sat, May 13, 2023 9:33 AM UTC	172.20.21.1		4848																																												
CN=wmeta3	56A7E2781A0CFE884B83AF533EB014D1	Fri, Nov 19, 2021 1:37 AM UTC	Sat, May 21, 2022 12:37 AM UTC	172.20.21.1		3389																																												

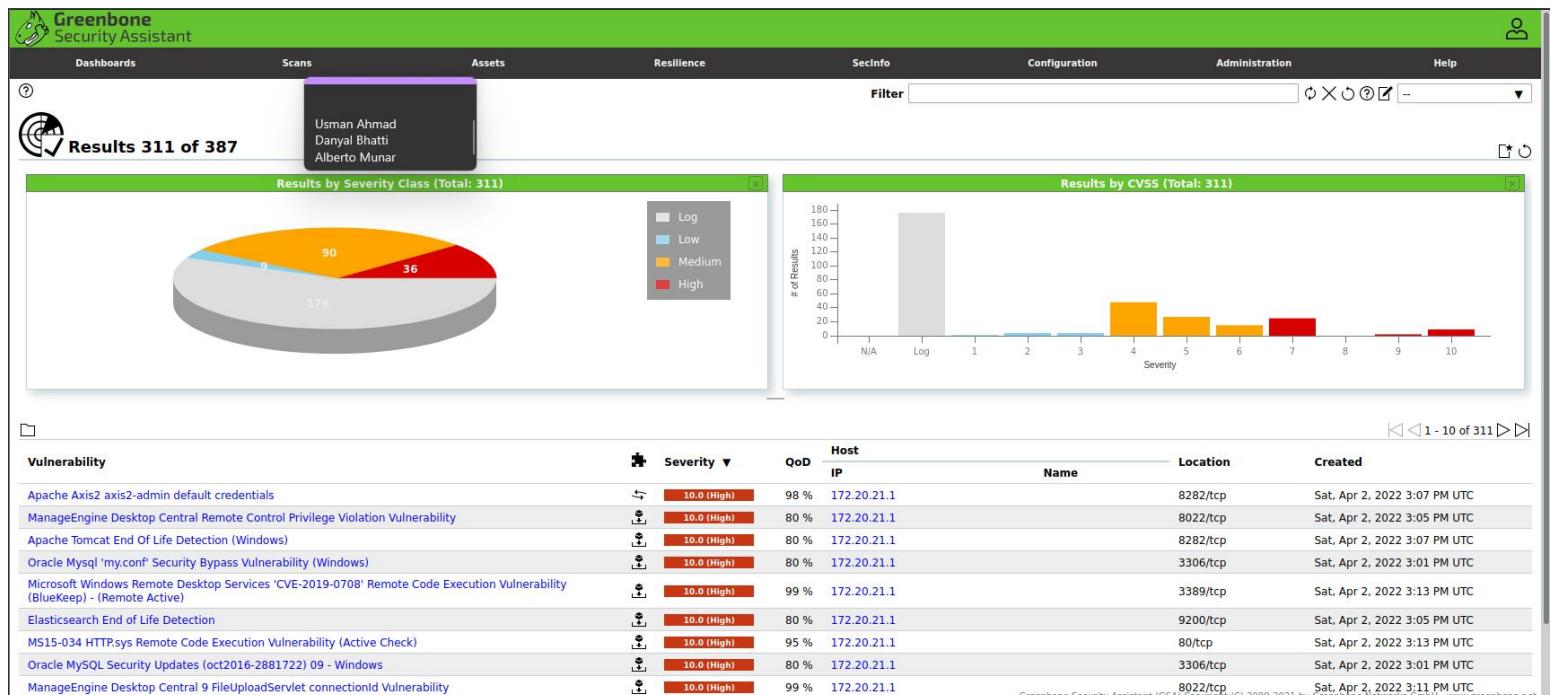
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

The total Report for the scan of the Network:



All The Vulnerabilities by class:



Pings

The above Screenshots are all the Vulnerabilities that were found on the systems that were

Pinging All Machines:

```
[srt411@m1-g9-sec ~]$ ping 172.20.19.2
PING 172.20.19.2 (172.20.19.2) 56(84) bytes of data.
64 bytes from 172.20.19.2: icmp_seq=1 ttl=128 time=0.423 ms
64 bytes from 172.20.19.2: icmp_seq=2 ttl=128 time=0.298 ms
^C
--- 172.20.19.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1035ms
rtt min/avg/max/mdev = 0.298/0.360/0.423/0.065 ms
[srt411@m1-g9-sec ~]$ ping 172.20.19.3
PING 172.20.19.3 (172.20.19.3) 56(84) bytes of data.
64 bytes from 172.20.19.3: icmp_seq=1 ttl=64 time=0.486 ms
64 bytes from 172.20.19.3: icmp_seq=2 ttl=64 time=0.273 ms
^C
--- 172.20.19.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.273/0.379/0.486/0.108 ms
[srt411@m1-g9-sec ~]$ ping 172.20.19.4
PING 172.20.19.4 (172.20.19.4) 56(84) bytes of data.
64 bytes from 172.20.19.4: icmp_seq=1 ttl=64 time=0.475 ms
64 bytes from 172.20.19.4: icmp_seq=2 ttl=64 time=0.258 ms
^C
--- 172.20.19.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1047ms
rtt min/avg/max/mdev = 0.258/0.366/0.475/0.110 ms
[srt411@m1-g9-sec ~]$ ping 172.20.19.5
PING 172.20.19.5 (172.20.19.5) 56(84) bytes of data.
64 bytes from 172.20.19.5: icmp_seq=1 ttl=128 time=0.386 ms
64 bytes from 172.20.19.5: icmp_seq=2 ttl=128 time=0.281 ms
^C
--- 172.20.19.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1021ms
rtt min/avg/max/mdev = 0.281/0.333/0.386/0.055 ms
[srt411@m1-g9-sec ~]$ ping 172.20.19.10
PING 172.20.19.10 (172.20.19.10) 56(84) bytes of data.
64 bytes from 172.20.19.10: icmp_seq=1 ttl=64 time=0.354 ms
64 bytes from 172.20.19.10: icmp_seq=2 ttl=64 time=0.251 ms
^C
--- 172.20.19.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1027ms
rtt min/avg/max/mdev = 0.251/0.302/0.354/0.054 ms
[srt411@m1-g9-sec ~]$ _
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

Snort:

Snort Configuration:

The snort file can be configured with:

vim /etc/snort/snort.conf

```
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
#
# Step #1: Set the network variables. For more information, see README.variables
#####
#
# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET

# List of sip servers on your network
ipvar SIP_SERVERS $HOME_NET

# List of ports you run web servers on
portvar HTTP_PORTS !80,81,311,383,591,593,981,1220,1414,1741,1830,2301,2381,2809,3837,3128,3782,4343,4848,5250,6988,7000,7001,71
44,7145,7510,7777,7729,8800,8808,8814,8828,8868,8888,8890,8118,8123,8180,8181,8243,8280,8308,8800,8888,8899,9000,9060,9000,
9898,9891,9443,9999,11371,34443,34444,41000,50002,55551

# List of ports you want to look for SHELLCODE on.
portvar SHELLCODE_PORTS !80

# List of ports you might see oracle attacks on
```

75,1

5x

Usman Ahmad
Danyal Bhatti
Alberto Munar

ipvar HOME_NET was set to any so that all the IPs on the network could be picked up.

```
#####
#
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####
#
# site specific rules
include $RULE_PATH/local.rules

#include $RULE_PATH/community-rules/
#include $RULE_PATH/community-rules/community.rules
#include $RULE_PATH/local.rules
#include $RULE_PATH/app-detect.rules
#include $RULE_PATH/attack-responses.rules
#include $RULE_PATH/backdoor.rules
#include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

The site-specific rules were described in the local rules file.

Snort Rules:

The following are the snort rules that we set up for collecting logs and traffic from all the interfaces.

```
GNU nano 2.9.8                               /etc/snort/rules/local.rules

alert icmp any any -> $HOME_NET any (msg:"ICMP"; sid:1000001; rev:1; classtype:icmp-event; detection_filter:track by_dst, count 1, interval 10, threshold 1, type both;)
alert tcp any any -> $HOME_NET 21 (msg:"FTP protocol usage"; sid:1000002; rev:1;)
alert tcp any any -> $HOME_NET 80 (msg:"HTTP protocol usage"; sid:1000003; rev:1;)
alert tcp any any -> $HOME_NET 80 (flags: S; msg:"DDOS"; flow: stateless; threshold: type both, track by_dst, count 70, seconds 1;)
alert tcp any any -> $HOME_NET 22 (msg: "NMAP TCP";sid:1000005; rev:2;)
alert tcp any any -> $HOME_NET 22 (msg:"SSH"; flow:to_server,established; content:"SSH-";metadata:service ssh; classtype:misc-audit; sid:1000006; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"ssh login"; flow:established, to_server; content:"ssh "; sid:10000001; rev:1;)
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

nmap scan snort test:

```
(kali㉿kali-g9-s5)~]$ sudo nmap -sT -p22 172.20.19.1
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 08:28 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.20.19.1
Host is up (0.00039s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:50:56:BA:EA:B4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
(kali㉿kali-g9-s5)~]$
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

```

| DFA
|   1 byte states : 1.56
|   2 byte states : 0.00
|   4 byte states : 0.00
+-----
[ Number of patterns truncated to 20 bytes: 0 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens192".
Reload thread starting...
Reload thread started, thread 0x7f34b68c2700 (6940)
Decoding Ethernet
Set gid to 1001
Set uid to 1001

==== Initialization Complete ====

,-> Snort! <-*
  Version 2.9.19 GRE (Build 85)
  By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
  Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
  Copyright (C) 1998-2013 Sourcefire, Inc., et al.
  Using libpcap version 1.9.1 (with TPACKET_V3)
  Using PCRE version: 8.42 2018-03-20
  Using ZLIB version: 1.2.11

  Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
  Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
  Preprocessor Object: SF_SIP Version 1.1 <Build 1>
  Preprocessor Object: SF_SDF Version 1.1 <Build 1>
  Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
  Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
  Preprocessor Object: SF_POP Version 1.0 <Build 1>
  Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
  Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
  Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
  Preprocessor Object: SF_GTP Version 1.1 <Build 1>
  Preprocessor Object: SF_SSH Version 1.1 <Build 3>
  Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
  Preprocessor Object: SF_DNS Version 1.1 <Build 4>
  Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
  Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

Commencing packet processing (pid=6935)
04/03/08:28:11.914649 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 172.20.19.10:33900 -> 172.20.19.1:80
04/03/08:28:28.040988 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 172.20.19.10:33902 -> 172.20.19.1:80
04/03/08:28:49.268771 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55666 -> 172.20.19.1:22
04/03/08:28:49.269038 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55666 -> 172.20.19.1:22
04/03/08:28:49.269084 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55666 -> 172.20.19.1:22

```

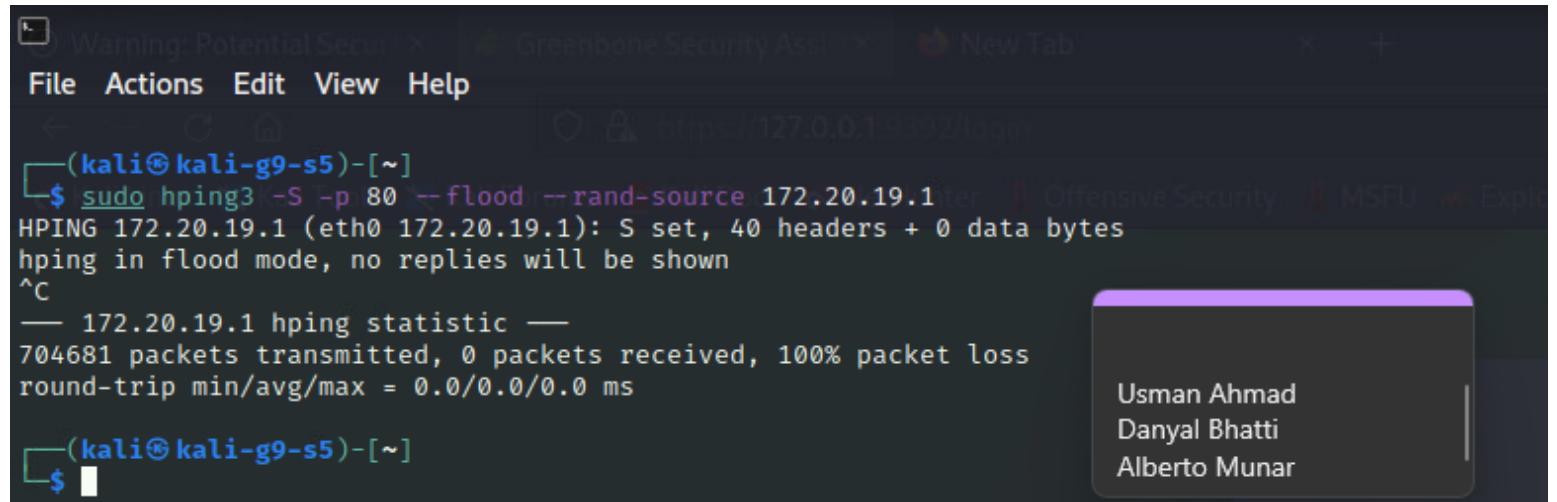
Usman Ahmad
Danyal Bhatti
Alberto Munar

The image below shows the event or the activity that was collected by performing an nmap scan.

Attacks:

DDoS or DoS attack:

A tool called hping3 was used to flood a system with SYN packets:



The screenshot shows a terminal window on a Kali Linux VM. The terminal title is '(kali㉿kali-g9-s5)'. The user runs the command `sudo hping3 -S -p 80 --flood --rand-source 172.20.19.1`. The output indicates that 704681 packets were transmitted to the target at port 80, resulting in 100% packet loss. A tooltip in the bottom right corner lists three names: Usman Ahmad, Danyal Bhatti, and Alberto Munar.

```
(kali㉿kali-g9-s5)~$ sudo hping3 -S -p 80 --flood --rand-source 172.20.19.1
HPING 172.20.19.1 (eth0 172.20.19.1): S set, 40 headers + 0 data bytes
hpPing in flood mode, no replies will be shown
^C
-- 172.20.19.1 hping statistic --
704681 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali㉿kali-g9-s5)~$
```

Hping is essentially flooding the target VM with SYN packets.

Snort event Logging for DoS attack:

```
04/03-08:54:47.428335 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 231.127.83.199:25743 -> 172.20.19.1:80
04/03-08:54:47.428338 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 20.185.27.174:25738 -> 172.20.19.1:80
04/03-08:54:47.428339 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 167.127.50.59:25751 -> 172.20.19.1:80
04/03-08:54:47.428343 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 23.288.1.61:25745 -> 172.20.19.1:80
04/03-08:54:47.428344 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 174.59.1.27:25750 -> 172.20.19.1:80
04/03-08:54:47.428349 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 12.141.234.116:25721 -> 172.20.19.1:80
04/03-08:54:47.428353 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 50.20.127.153:25734 -> 172.20.19.1:80
04/03-08:54:47.428358 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 238.117.79.174:25744 -> 172.20.19.1:80
04/03-08:54:47.428363 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 237.98.47.180:25749 -> 172.20.19.1:80
04/03-08:54:47.428438 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 190.139.161.232:25717 -> 172.20.19.1:80
04/03-08:54:47.428458 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 235.72.199.238:25719 -> 172.20.19.1:80
04/03-08:54:47.428459 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 183.211.76.67:25740 -> 172.20.19.1:80
04/03-08:54:47.428458 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 76.230.226.36:25754 -> 172.20.19.1:80
04/03-08:54:47.428462 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 90.37.197.23:25725 -> 172.20.19.1:80
04/03-08:54:47.428466 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 168.247.217.234:25757 -> 172.20.19.1:80
04/03-08:54:47.428468 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 217.211.211.39:25737 -> 172.20.19.1:80
04/03-08:54:47.428471 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 23.37.191.114:25725 -> 172.20.19.1:80
04/03-08:54:47.428473 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 9.195.280.195:25742 -> 172.20.19.1:80
04/03-08:54:47.428477 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 100.127.13.91:25753 -> 172.20.19.1:80
04/03-08:54:47.428478 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 237.134.191.180:25720 -> 172.20.19.1:80
04/03-08:54:47.428482 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 187.37.241.134:25762 -> 172.20.19.1:80
04/03-08:54:47.428483 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 138.205.54.58:25755 -> 172.20.19.1:80
04/03-08:54:47.428487 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 248.43.16.148:25767 -> 172.20.19.1:80
04/03-08:54:47.428488 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 126.83.98.27:25763 -> 172.20.19.1:80
04/03-08:54:47.428492 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 116.81.199.101:25772 -> 172.20.19.1:80
04/03-08:54:47.428492 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 34.67.129.72:25776 -> 172.20.19.1:80
04/03-08:54:47.428498 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 211.206.166.75:25782 -> 172.20.19.1:80
04/03-08:54:47.428502 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 197.168.251.238:25752 -> 172.20.19.1:80
04/03-08:54:47.428502 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 72.97.251.187:25761 -> 172.20.19.1:80
04/03-08:54:47.428587 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 238.174.116.161:25777 -> 172.20.19.1:80
04/03-08:54:47.428511 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 241.127.54.229:25778 -> 172.20.19.1:80
04/03-08:54:47.428516 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 68.199.86.153:25758 -> 172.20.19.1:80
04/03-08:54:47.428521 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 248.37.247.155:25764 -> 172.20.19.1:80
04/03-08:54:47.428525 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 125.185.101.104:25766 -> 172.20.19.1:80
04/03-08:54:47.428529 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 37.285.58.170:25759 -> 172.20.19.1:80
04/03-08:54:47.428631 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 43.54.34.52:25765 -> 172.20.19.1:80
04/03-08:54:47.428534 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 71.285.235.116:25768 -> 172.20.19.1:80
04/03-08:54:47.428538 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 76.79.127.43:25769 -> 172.20.19.1:80
04/03-08:54:47.428615 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 47.27.226.52:25770 -> 172.20.19.1:80
04/03-08:54:47.428622 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 52.99.20.100:25779 -> 172.20.19.1:80
04/03-08:54:47.428627 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 199.153.79.49:25780 -> 172.20.19.1:80
04/03-08:54:47.428631 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 21.211.59.197:25774 -> 172.20.19.1:80
04/03-08:54:47.428632 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 21.211.59.197:25774 -> 172.20.19.1:80
04/03-08:54:47.428635 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 150.52.27.229:25773 -> 172.20.19.1:80
04/03-08:54:47.428639 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 52.150.0.150:25771 -> 172.20.19.1:80
04/03-08:54:47.428648 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 166.5.125.200:25790 -> 172.20.19.1:80
04/03-08:54:47.428644 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 39.181.16.47:25781 -> 172.20.19.1:80
04/03-08:54:47.428645 [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 61.134.13.37:25792 -> 172.20.19.1:80
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

SSH Logins and Brute Force Attacks:

```
(kali㉿kali-g9-s5) [~]
$ sudo hydra -l srt411 -P /usr/share/wordlists/rockyou.txt 172.20.19.1 ssh -MFU -Elog=BB -QHDS
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-03 09:03:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1:p:14344400), ~896525 tries per task
[DATA] attacking ssh://172.20.19.1:22/
[22][ssh] host: 172.20.19.1 login: srt411 password: srt411
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-03 09:03:09
```

1 ⓘ

Usman Ahmad
Danyal Bhatti
Alberto Munar

```
(kali㉿kali-g9-s5) [~]
$
```

1 ⓘ

Snort Logs and events triggered by SSH Brute force

```
Using ZLIB version: 1.2.11

Rules Engine: SF_SMORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

Commencing packet processing (pid=7131)
04/03/09:07:57.520715 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55752 -> 172.2
0.19.1:22
04/03/09:07:57.817217 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55758 -> 172.2
0.19.1:22
04/03/09:07:57.817017 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55766 -> 172.2
0.19.1:22
04/03/09:07:57.816758 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55754 -> 172.2
0.19.1:22
04/03/09:07:57.817048 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55770 -> 172.2
0.19.1:22
04/03/09:07:57.817173 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55768 -> 172.2
0.19.1:22
04/03/09:07:57.817392 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55786 -> 172.2
0.19.1:22
04/03/09:07:57.817602 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55788 -> 172.2
0.19.1:22
04/03/09:07:57.817413 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55756 -> 172.2
0.19.1:22
04/03/09:07:57.817277 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55776 -> 172.2
0.19.1:22
04/03/09:07:57.817140 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55778 -> 172.2
0.19.1:22
04/03/09:07:57.817342 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55772 -> 172.2
0.19.1:22
04/03/09:07:57.816872 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55774 -> 172.2
0.19.1:22
04/03/09:07:57.817690 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.10:55790 -> 172.2
0.19.1:22
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

SSH Connection:

```
[srt411@m4-g9-sec ~]$ ssh srt411@172.20.19.1
srt411@172.20.19.1's password:
Last login: Sun Apr  3 09:19:43 2022 from 172.20.19.4
[srt411@m1-g9-sec ~]$ █
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

Snort Pick up of ssh connection:

```
| Memory (KB)      : 14.81
| Pattern         : 0.17
| Match Lists    : 0.23
| DFA
|   1 byte states : 1.56
|   2 byte states : 0.00
|   4 byte states : 0.00
+-----[ Number of patterns truncated to 20 bytes: 0 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens192".
Reload thread starting...
Reload thread started, thread 0x7f6d89dae700 (7281)
Decoding Ethernet
Set gid to 1001
Set uid to 1001

---- Initialization Complete ----

--> Snort! <--
Version 2.9.19 GRE (Build 85)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.9.1 (with TPACKET_V3)
Using PCRE version: 8.42 2018-03-20
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SFCCPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

Commencing packet processing (pid=7276)
04/03/09:19:59.242209 [**] [1:19559:5] SSH [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.20.19.4:41160 -> 172.20.19.1:22
-
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

Deep Scan of M1 of each port service and details:

```
(kali㉿kali-g9-s5) [~]
$ sudo nmap -p- -sV -o 172.20.19.1 --system-dns
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 10:10 EDT
Nmap scan report for 172.20.19.1
Host is up (0.00031s latency).
Not shown: 65386 filtered tcp ports (no-response), 147 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0 (protocol 2.0)
9090/tcp  closed zeus-admin
MAC Address: 00:50:56:BA:EA:B4 (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.1
OS details: Linux 5.1
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 143.28 seconds
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

Snort collection of data:

```
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FFTTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=7997)
04/03-10:10:42.978877 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:35556 -> 172.20.19.1:22
04/03-10:10:42.979225 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:35556 -> 172.20.19.1:22
04/03-10:10:42.979257 [**] [1:1000002:1] FTP protocol usage [**] [Priority: 0] {TCP} 172.20.19.10:35556 -> 172.20.19.1:21
04/03-10:10:42.981463 [**] [1:1000003:1] HTTP protocol usage [**] [Priority: 0] {TCP} 172.20.19.10:35556 -> 172.20.19.1:80
04/03-10:10:44.000405 [**] [1:1000003:1] HTTP protocol usage [**] [Priority: 0] {TCP} 172.20.19.10:35558 -> 172.20.19.1:80
04/03-10:10:44.000499 [**] [1:1000002:1] FTP protocol usage [**] [Priority: 0] {TCP} 172.20.19.10:35558 -> 172.20.19.1:21
04/03-10:13:04.172587 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.173029 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.191453 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.191970 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.193683 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.292233 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45807 -> 172.20.19.1:22
04/03-10:13:04.292631 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45807 -> 172.20.19.1:22
04/03-10:13:04.392316 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45808 -> 172.20.19.1:22
04/03-10:13:04.392660 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45808 -> 172.20.19.1:22
04/03-10:13:04.492372 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45809 -> 172.20.19.1:22
04/03-10:13:04.492628 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45809 -> 172.20.19.1:22
04/03-10:13:04.592448 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45810 -> 172.20.19.1:22
04/03-10:13:04.592686 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45810 -> 172.20.19.1:22
04/03-10:13:04.692543 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45811 -> 172.20.19.1:22
04/03-10:13:04.692743 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45811 -> 172.20.19.1:22
04/03-10:13:04.792650 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45812 -> 172.20.19.1:22
04/03-10:13:04.792943 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45812 -> 172.20.19.1:22
04/03-10:13:04.892970 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45819 -> 172.20.19.1:22
04/03-10:13:04.893271 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45819 -> 172.20.19.1:22
04/03-10:13:04.918831 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45821 -> 172.20.19.1:22
04/03-10:13:04.943179 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45822 -> 172.20.19.1:22
04/03-10:13:04.968264 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45823 -> 172.20.19.1:22
04/03-10:13:05.095816 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45821 -> 172.20.19.1:22
04/03-10:13:05.120075 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45822 -> 172.20.19.1:22
04/03-10:13:05.195325 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45821 -> 172.20.19.1:22
04/03-10:13:05.220469 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45822 -> 172.20.19.1:22
04/03-10:13:05.295702 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45821 -> 172.20.19.1:22
04/03-10:13:05.320825 [**] [1:1000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45822 -> 172.20.19.1:22
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

Security Goals, Vulnerabilities and Threats

The goal is to protect the network infrastructure and always keep the resources accessible and effective as much as possible. Due to the vast number of resources, services and the design of the network and devices, it is not possible to eliminate threats. Due to the vast number of software programs and application services that are present regardless of how secure the network may be configured, there will be openings and vulnerabilities that can be exploited to get access to the network and perform kinds of attacks and malicious goals of adversaries. The goal is to keep track of the network activities and unusual activities that may take place, which can be found with snort and then further mitigate those issues by looking at demographics that could further help the businesses and other infrastructures.

How Data Collection help you achieve your goal:

Data Collection allows us to keep track and get the understanding of the events and activities that are taking place. These further help with, getting to know the unusual activities that are likely threats, track them down and protect the infrastructure by mitigating the threats

Explain Data Collection:

The collection of activities and events that take place in a network and collecting all that information and preserving or importing it in a readable format for visual or statistical analysis is basically data collection. For our case we sent the Snort Files to Kali from M1, we also collected packet captures in the form of CSV and the vulnerability report in CSV.

Data Collection:

Brute Force Attack:

The following screenshot shows the data imported in csv format.

No.	Time	Source	Destinatic Protocol	Length	Info
1	0 172.20.19. 172.20.19. TCP			74	55796 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=2679135521 TSectr=0 WS=128
2	0.000476 172.20.19. 172.20.19. TCP			74	22 > 55796 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TStamp=2679135521 TSectr=2679135521 WS=128
3	0.000511 172.20.19. 172.20.19. TCP			66	55796 > 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2679135521 TSectr=2679135521 WS=128
4	0.000539 172.20.19. 172.20.19. SSHv2			88	Client: Protocol (SSH-2.0-libssh_0.9.6)
5	0.000663 172.20.19. 172.20.19. TCP			66	22 > 55796 [ACK] Seq=1 Ack=23 Win=29056 Len=0 TStamp=2679135522 TSectr=2679135522
6	0.016011 172.20.19. 172.20.19. SSHv2			87	Server: Protocol (SSH-2.0-OpenSSH_8.0)
7	0.016021 172.20.19. 172.20.19. TCP			66	55796 > 22 [ACK] Seq=23 Ack=22 Win=64256 Len=0 TStamp=2679135537 TSectr=2679135537
8	0.016216 172.20.19. 172.20.19. SSHv2			1042	Client: Key Exchange Init
9	0.018577 172.20.19. 172.20.19. SSHv2			1114	Server: Key Exchange Init
10	0.018596 172.20.19. 172.20.19. TCP			66	55796 > 22 [ACK] Seq=999 Ack=1070 Win=64128 Len=0 TStamp=2679135540 TSectr=2679135540
11	0.018772 172.20.19. 172.20.19. SSHv2			114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
12	0.025803 172.20.19. 172.20.19. SSHv2			454	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=180)
13	0.025816 172.20.19. 172.20.19. TCP			66	55796 > 22 [ACK] Seq=1047 Ack=1458 Win=64128 Len=0 TStamp=2679135547 TSectr=2679135531
14	0.026026 172.20.19. 172.20.19. SSHv2			82	Client: New Keys
15	0.067070 172.20.19. 172.20.19. TCP			66	22 > 55796 [ACK] Seq=1458 Ack=1063 Win=30976 Len=0 TStamp=267913570373 TSectr=2679135547
16	0.067086 172.20.19. 172.20.19. SSHv2			118	Client: Encrypted packet (len=52)
17	0.067188 172.20.19. 172.20.19. TCP			66	22 > 55796 [ACK] Seq=1458 Ack=1115 Win=30976 Len=0 TStamp=267913570373 TSectr=2679135588
18	0.067261 172.20.19. 172.20.19. SSHv2			118	Server: Encrypted packet (len=52)
19	0.067266 172.20.19. 172.20.19. TCP			66	55796 > 22 [ACK] Seq=1115 Ack=1510 Win=64128 Len=0 TStamp=2679135588 TSectr=267913570373
20	0.06735 172.20.19. 172.20.19. SSHv2			134	Client: Encrypted packet (len=68)
21	0.074651 172.20.19. 172.20.19. SSHv2			150	Server: Encrypted packet (len=84)
22	0.074733 172.20.19. 172.20.19. SSHv2			118	Client: Encrypted packet (len=52)
23	0.074765 172.20.19. 172.20.19. TCP			66	55796 > 22 [FIN, ACK] Seq=1235 Ack=1594 Win=64128 Len=0 TStamp=2679135596 TSectr=267913570380
24	0.078086 172.20.19. 172.20.19. TCP			66	22 > 55796 [FIN, ACK] Seq=1594 Ack=1236 Win=30976 Len=0 TStamp=2679135596 TSectr=2679135596
25	0.078098 172.20.19. 172.20.19. TCP			66	55796 > 22 [ACK] Seq=1236 Ack=1595 Win=64128 Len=0 TStamp=2679135599 TSectr=267913570384
26	0.30867 172.20.19. 172.20.19. TCP			74	55800 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=2679135830 TSectr=0 WS=128
27	0.308704 172.20.19. 172.20.19. TCP			74	55798 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=2679135830 TSectr=0 WS=128
28	0.308969 172.20.19. 172.20.19. TCP			74	22 > 55800 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TStamp=2679135830 WS=128
29	0.30898 172.20.19. 172.20.19. TCP			66	55800 > 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2679135830 TSectr=267913570614
30	0.309001 172.20.19. 172.20.19. TCP			74	22 > 55798 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TStamp=2679135830 TSectr=2679135830 WS=128
31	0.309016 172.20.19. 172.20.19. TCP			66	55798 > 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=2679135830 TSectr=267913570614
32	0.309044 172.20.19. 172.20.19. TCP			74	55802 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=2679135830 TSectr=0 WS=128
33	0.30905 172.20.19. 172.20.19. SSHv2			88	Client: Protocol (SSH-2.0-libssh_0.9.6)
34	0.30909 172.20.19. 172.20.19. SSHv2			88	Client: Protocol (SSH-2.0-libssh_0.9.6)
35	0.309098 172.20.19. 172.20.19. TCP			71	55804 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=2679135830 TSectr=0 WS=128

Usman Ahmad
Danyal Bhatti
Alberto Munar

DDoS Attack:

The following data was collected with DDoS attack:

No.	Time	Source	Destinatic	Protocol	Length	Info
1	0	145.131.82	172.20.19.	TCP	54	1911 > 80 [SYN] Seq=0 Win=512 Len=0
2	5.47E-05	63.21.131. 172.20.19.	TCP		54	1912 > 80 [SYN] Seq=0 Win=512 Len=0
3	7.01E-05	137.238.18	172.20.19.	TCP	54	1913 > 80 [SYN] Seq=0 Win=512 Len=0
4	8.37E-05	239.213.23	172.20.19.	TCP	54	1914 > 80 [SYN] Seq=0 Win=512 Len=0
5	9.85E-05	92.188.92. 172.20.19.	TCP		54	1915 > 80 [SYN] Seq=0 Win=512 Len=0
6	0.000122	120.139.50	172.20.19.	TCP	54	1916 > 80 [SYN] Seq=0 Win=512 Len=0
7	0.000135	162.214.16	172.20.19.	TCP	54	1917 > 80 [SYN] Seq=0 Win=512 Len=0
8	0.000147	174.196.16	172.20.19.	TCP	54	1918 > 80 [SYN] Seq=0 Win=512 Len=0
9	0.00016	160.71.24.	172.20.19.	TCP	54	1919 > 80 [SYN] Seq=0 Win=512 Len=0
10	0.000172	88.57.213.	172.20.19.	TCP	54	1920 > 80 [SYN] Seq=0 Win=512 Len=0
11	0.000184	69.239.17	172.20.19.	TCP	54	1921 > 80 [SYN] Seq=0 Win=512 Len=0
12	0.000196	31.162.120	172.20.19.	TCP	54	1922 > 80 [SYN] Seq=0 Win=512 Len=0
13	0.000209	57.97.99.1	172.20.19.	TCP	54	1923 > 80 [SYN] Seq=0 Win=512 Len=0
14	0.000229	62.172.9.1	172.20.19.	TCP	54	1924 > 80 [SYN] Seq=0 Win=512 Len=0
15	0.000241	196.26.118	172.20.19.	TCP	54	1925 > 80 [SYN] Seq=0 Win=512 Len=0
16	0.000254	149.67.38.	172.20.19.	TCP	54	1926 > 80 [SYN] Seq=0 Win=512 Len=0
17	0.000266	122.175.20	172.20.19.	TCP	54	1927 > 80 [SYN] Seq=0 Win=512 Len=0
18	0.000287	117.32.224	172.20.19.	TCP	54	1928 > 80 [SYN] Seq=0 Win=512 Len=0
19	0.000301	245.188.73	172.20.19.	TCP	54	1929 > 80 [SYN] Seq=0 Win=512 Len=0
20	0.00032	38.62.191.	172.20.19.	TCP	54	1930 > 80 [SYN] Seq=0 Win=512 Len=0
21	0.00034	206.50.122	172.20.19.	TCP	54	1931 > 80 [SYN] Seq=0 Win=512 Len=0
22	0.000353	75.22.210.	172.20.19.	TCP	54	1932 > 80 [SYN] Seq=0 Win=512 Len=0
23	0.000366	149.182.22	172.20.19.	TCP	54	1933 > 80 [SYN] Seq=0 Win=512 Len=0
24	0.000378	9.64.112.1	172.20.19.	TCP	54	1934 > 80 [SYN] Seq=0 Win=512 Len=0
25	0.000384	15.57.14.1	172.20.19.	TCP	54	1935 > 80 [SYN] Seq=0 Win=512 Len=0
26	0.000397	160.148.111	172.20.19.	TCP	54	1936 > 80 [SYN] Seq=0 Win=512 Len=0
27	0.000409	19.203.46.	172.20.19.	TCP	54	1937 > 80 [SYN] Seq=0 Win=512 Len=0
28	0.000426	214.62.24.	172.20.19.	TCP	54	1938 > 80 [SYN] Seq=0 Win=512 Len=0
29	0.000439	147.73.49.	172.20.19.	TCP	54	1939 > 80 [SYN] Seq=0 Win=512 Len=0
30	0.000451	96.66.110.	172.20.19.	TCP	54	1940 > 80 [SYN] Seq=0 Win=512 Len=0
31	0.000464	68.94.66.1	172.20.19.	TCP	54	1941 > 80 [SYN] Seq=0 Win=512 Len=0
32	0.000476	168.72.106	172.20.19.	TCP	54	1942 > 80 [SYN] Seq=0 Win=512 Len=0
33	0.000495	63.81.159.	172.20.19.	TCP	54	1943 > 80 [SYN] Seq=0 Win=512 Len=0
34	0.000513	228.21.132	172.20.19.	TCP	54	1944 > 80 [SYN] Seq=0 Win=512 Len=0
35	0.000525	122.208.65	172.20.19.	TCP	54	1945 > 80 [SYN] Seq=0 Win=512 Len=0

Usman Ahmad
Danyal Bhatti
Alberto Munar

Nmap Scan:

The following Data was generated with Nmap scan:

No.	Time	Source	Destinatic Protocol	Length	Info
1	0	VMware	_Broadcast ARP	42	Who has 172.20.21.1? Tell 172.20.21.10
2	3.61E-05	VMware	_Broadcast ARP	42	Who has 172.20.21.2? Tell 172.20.21.10
3	4.04E-05	VMware	_Broadcast ARP	42	Who has 172.20.21.3? Tell 172.20.21.10
4	6.72E-05	VMware	_Broadcast ARP	42	Who has 172.20.21.4? Tell 172.20.21.10
5	7.09E-05	VMware	_Broadcast ARP	42	Who has 172.20.21.5? Tell 172.20.21.10
6	7.48E-05	VMware	_Broadcast ARP	42	Who has 172.20.21.6? Tell 172.20.21.10
7	7.89E-05	VMware	_Broadcast ARP	42	Who has 172.20.21.7? Tell 172.20.21.10
8	9.04E-05	VMware	_Broadcast ARP	42	Who has 172.20.21.8? Tell 172.20.21.10
9	9.52E-05	VMware	_Broadcast ARP	42	Who has 172.20.21.9? Tell 172.20.21.10
10	0.000101	VMware	_Broadcast ARP	42	Who has 172.20.21.11? Tell 172.20.21.10
11	0.000223	VMware	_VMware _ARP	60	172.20.21.1 is at 00:50:56:ba:a5:ce
12	0.000337	VMware	_VMware _ARP	60	172.20.21.2 is at 00:50:56:ba:74:7f
13	0.000596	VMware	_VMware _ARP	60	172.20.21.3 is at 00:50:56:ba:fc:be
14	0.018041	VMware	_Broadcast ARP	42	Who has 172.20.21.14? Tell 172.20.21.10
15	0.018068	VMware	_Broadcast ARP	42	Who has 172.20.21.15? Tell 172.20.21.10
16	0.018078	VMware	_Broadcast ARP	42	Who has 172.20.21.16? Tell 172.20.21.10
17	0.018082	VMware	_Broadcast ARP	42	Who has 172.20.21.17? Tell 172.20.21.10
18	0.018085	VMware	_Broadcast ARP	42	Who has 172.20.21.18? Tell 172.20.21.10
19	0.018088	VMware	_Broadcast ARP	42	Who has 172.20.21.19? Tell 172.20.21.10
20	0.100303	VMware	_Broadcast ARP	42	Who has 172.20.21.22? Tell 172.20.21.10
21	0.100334	VMware	_Broadcast ARP	42	Who has 172.20.21.23? Tell 172.20.21.10
22	0.100359	VMware	_Broadcast ARP	42	Who has 172.20.21.24? Tell 172.20.21.10
23	0.100365	VMware	_Broadcast ARP	42	Who has 172.20.21.25? Tell 172.20.21.10
24	0.10037	VMware	_Broadcast ARP	42	Who has 172.20.21.26? Tell 172.20.21.10
25	0.100373	VMware	_Broadcast ARP	42	Who has 172.20.21.27? Tell 172.20.21.10
26	0.100378	VMware	_Broadcast ARP	42	Who has 172.20.21.28? Tell 172.20.21.10
27	0.118188	VMware	_Broadcast ARP	42	Who has 172.20.21.31? Tell 172.20.21.10
28	0.11822	VMware	_Broadcast ARP	42	Who has 172.20.21.32? Tell 172.20.21.10
29	0.11823	VMware	_Broadcast ARP	42	Who has 172.20.21.33? Tell 172.20.21.10
30	0.118233	VMware	_Broadcast ARP	42	Who has 172.20.21.34? Tell 172.20.21.10
31	0.118238	VMware	_Broadcast ARP	42	Who has 172.20.21.35? Tell 172.20.21.10
32	0.118241	VMware	_Broadcast ARP	42	Who has 172.20.21.36? Tell 172.20.21.10
33	0.200498	VMware	_Broadcast ARP	42	Who has 172.20.21.39? Tell 172.20.21.10
34	0.200533	VMware	_Broadcast ARP	42	Who has 172.20.21.40? Tell 172.20.21.10
35	0.200556	VMware	_Broadcast ARP	42	Who has 172.20.21.41? Tell 172.20.21.10

Usman Ahmad
Danyal Bhatti
Alberto Munoz

Greenbone Scan Results:

Data collected after Greenbone Scan:

Snort Files/Logs collected and sent to Kali

```
boot.log-20220401 dnf.log maillog qemu-ga spooler-20220401
boot.log-20220403 dnf.log.1 maillog-20220102 samba spooler-20220403
btmp dnf.rpm.log maillog-20220109 secure sssd
bttmp-20220401 firewalld maillog-20220401 secure-20220102 tuned
chrony hawkey.log maillog-20220403 secure-20220109 vmware-network.1.log
[srt4110m1-g9-sec log]$/ zip -r snort.zip snort/
zip I/O error: Permission denied
zip error: Could not create output file (snort.zip)
[srt4110m1-g9-sec log]$/ sudo zip -r snort.zip snort/
adding: snort/ (stored 0%)
adding: snort/snort.log.1648788916 (deflated 69%)
adding: snort/snort.log.1648881858 (deflated 77%)
adding: snort/snort.log.1648954540 (stored 0%)
adding: snort/snort.log.1648955303 (stored 0%)
adding: snort/snort.log.1648955547 (stored 0%)
adding: snort/snort.log.1648955698 (deflated 66%)
adding: snort/snort.log.1648965894 (deflated 69%)
adding: snort/snort.log.1648965515 (deflated 68%)
adding: snort/snort.log.1648965717 (stored 0%)
adding: snort/snort.log.1648966109 (deflated 60%)
adding: snort/snort.log.1648976540 (deflated 43%)
adding: snort/snort.log.1648978762 (deflated 41%)
adding: snort/snort.log.1648979066 (deflated 60%)
adding: snort/snort.log.1648988889 (deflated 49%)
adding: snort/snort.log.1648990391 (deflated 60%)
adding: snort/snort.log.1648990480 (deflated 61%)
adding: snort/snort.log.1648998979 (deflated 79%)
adding: snort/snort.log.1648991272 (deflated 90%)
adding: snort/snort.log.1648991996 (deflated 68%)
adding: snort/snort.log.1648993281 (stored 0%)
adding: snort/snort.log.1648994745 (stored 0%)
adding: snort/snort.log.1648994969 (deflated 69%)
[srt4110m1-g9-sec log]$/ ls
anaconda cron hawkey.log-20220102 messages secure-20220401 vmware-network.1.log
audit cron-20220102 hawkey.log-20220109 messages-20220102 secure-20220403 vmware-network.2.log
boot.log cron-20220109 hawkey.log-20220401 messages-20220109 snot vmware-network.log
boot.log-20211207 cron-20220401 hawkey.log-20220403 messages-20220401 snort.zip vmware-vgauthsvc.log.0
boot.log-20211210 cron-20220403 kdump.log messages-20220403 spooler vmware-vmsvc-root.log
boot.log-20211215 dnf.librepo.log lastlog private spooler-20220102 vmware-vmtoolsd-root.log
boot.log-20220401 dnf.log maillog qemu-ga spooler-20220109 wtmp
boot.log-20220403 dnf.log.1 maillog-20220102 samba spooler-20220401
bttmp dnf.rpm.log maillog-20220109 secure spooler-20220403
bttmp-20220401 firewalld maillog-20220401 secure-20220102 sssd
chrony hawkey.log maillog-20220403 secure-20220109 tuned
[srt4110m1-g9-sec log]$/ scp snort.zip kali0172.20.19.10:/home/kali/Desktop
kali0172.20.19.10's password:
snort.zip
[srt4110m1-g9-sec log]$_
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

100% 2633KB 25.1MB/s 00:00

References

Chandel, R., says:, K. O. S. T. I. A. N. T. Y. N., says:, R. C., says:, A. A., & says:, V. (2022, January 12). *How to detect NMAP scan using Snort*. Hacking Articles. Retrieved April 4, 2022, from <https://www.hackingarticles.in/detect-nmap-scan-using-snort/>

Essche, A. V. (n.d.). *Re: Rule for detecting SSH*. Snort: Re: Rule for detecting ssh. Retrieved April 4, 2022, from <https://seclists.org/snort/2014/q2/482>

How to use SQLMAP to test a website for SQL injection vulnerability. GeeksforGeeks. (2021, June 28). Retrieved April 4, 2022, from <https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/>

Hydra: Kali linux tools. Kali Linux. (2022, February 10). Retrieved April 4, 2022, from <https://www.kali.org/tools/hydra/>

Shah, N. A. (I. C. via S.-users. (n.d.). *Snort rule to detect HTTP post data*. Snort: snort rule to detect HTTP POST data. Retrieved April 4, 2022, from <https://seclists.org/snort/2018/q1/317>

sinxLoud. (2019, January 22). *How to install DVWA into your linux distribution*. Medium. Retrieved April 4, 2022, from <https://medium.datadriveninvestor.com/setup-install-dvwa-into-your-linux-distribution-d76dc3b80357>

staff, J. R., Ruostemaa, J., Staff, Janne Ruostemaa Editor-in-chief and Technical writer at UpCloud since 2015. Cloud enthusiast writing about server technology and software., Editor-in-chief and Technical writer at UpCloud since 2015. Cloud enthusiast writing about server technology and software., Says:, B., says:, J. R., Says:, M., says:, J., says:, M. siraj, Says:, A., says:, S. M. S., says:, C. J., Says:, M., says:, J., says:, M. M., says:, I., says:, K., says:, A. D., ... says:, T. T. (2021, August 5). *How to install Snort on ubuntu*. UpCloud. Retrieved April 4, 2022, from <https://upcloud.com/community/tutorials/install-snort-ubuntu/>