Executive Summary

Responding to a Nation-State Cyber Attack

Udacity Project 2
December 2022

Roaa Alotaibi

Responding to a Nation-State Cyber Attack

- The National Peace Agency of North Udan managed to compromise a linux server which serves as a jump host to connect the Tridanium processing plant to the internet. They attempted to brute force the password of an employee account which triggered a security alarm. The security team have been immediately called onboard to respond to the security alarm and contain the ongoing cyberattack.

Threat Detection

- **Malware Scanning**

The below infected files have been identified on the server, after conducting a malware scanning using ClamAV:

```
/home/ubuntu/Downloads/ft32: Unix.Malware.Agent-6774375-0 FOUND
/home/ubuntu/Downloads/ft64: Unix.Malware.Agent-6774336-0 FOUND
/home/ubuntu/Downloads/wipefs: Unix.Tool.Miner-6443173-0 FOUND
```

Threat Detection

- **Malware Scanning**

Next, one more suspicious files is identified manually:

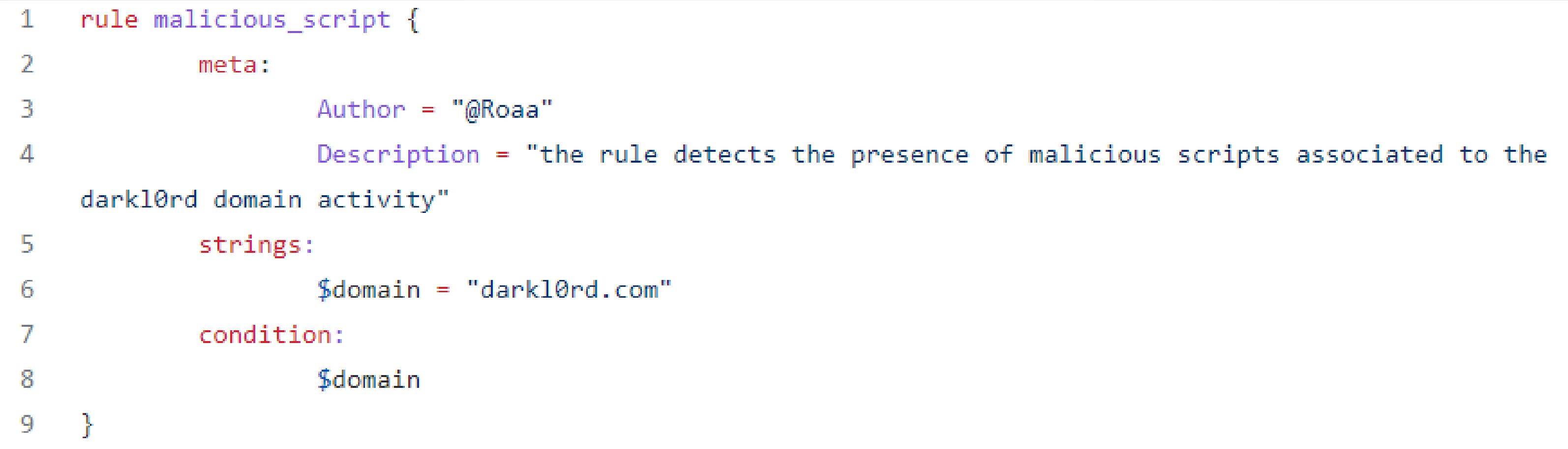
# Filename: SSH-One

This is a bash file which eliminates the firewall rules by turning them off, modifies the rc.local to run SSH-T & SSH-One malicious files when the system starts, it also has an embedded callout to: http://darkl0rd.com.

Threat Detection

- **Improved Defense**

After analyzing the manual identified suspicious file, I prepared a YARA rule to detect that malware, and to have a defense control against future threats.

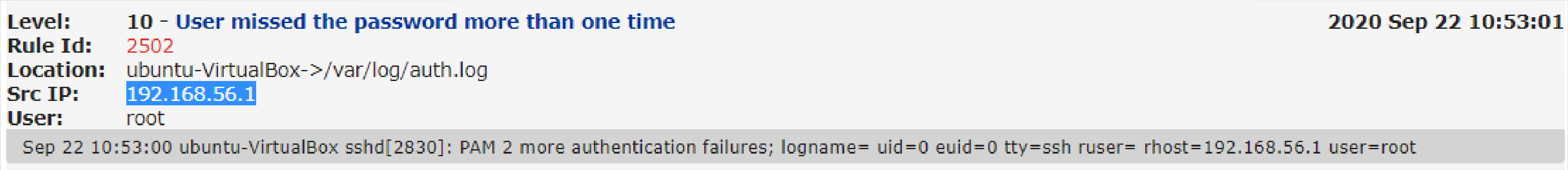


```
rule malicious_script {
        meta:
                Author = "@Roaa"
                Description = "the rule detects the presence of malicious scripts associated to the darkl0rd domain activity"
        strings:
                $domain = "darkl0rd.com"
        condition:
                $domain
}
```

Threat Mitigation

- **Attacker IP**

Using the Host-Based Intruder Detection System (HIDS) and through the means of OSSEC, the attacker IP address has been identified: 192.168.56.1

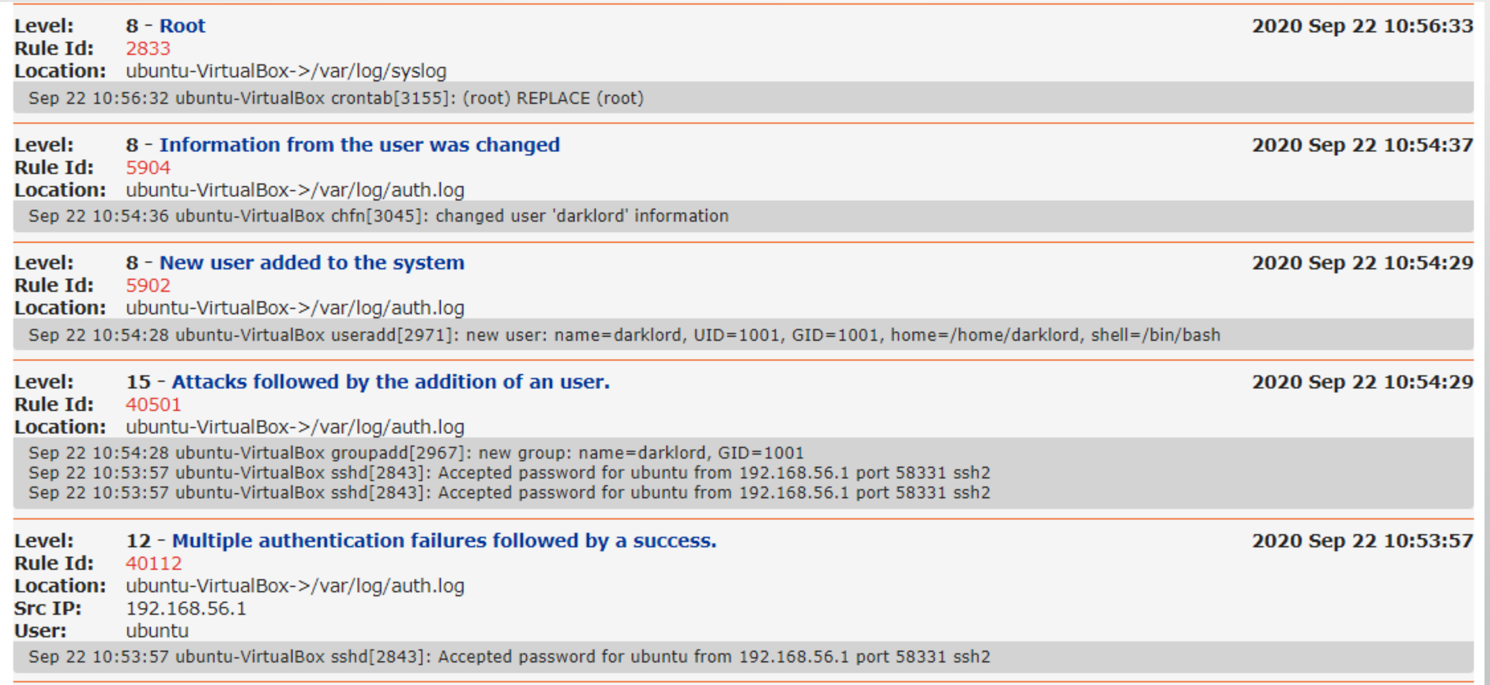


```
Level:     10 - User missed the password more than one time                                   2020 Sep 22 10:53:01
Rule Id:   2502
Location:  ubuntu-VirtualBox->/var/log/auth.log
Src IP:    192.168.56.1
User:      root
 Sep 22 10:53:00 ubuntu-VirtualBox sshd[2830]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1 user=root
```

Threat Mitigation

- **Backdoor Details**

Notably in OSSEC, the ubuntu user had multiple failed login attempts, changed UID to root, and created a new user named ‘darklord’ and a new group named ‘darklord’ and added the newly created user to that group.

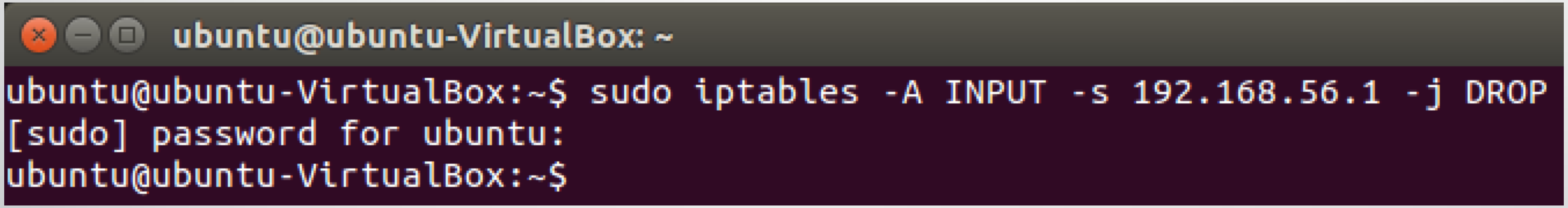


```
Level:      8 - Root                                                              2020 Sep 22 10:56:33
Rule Id:    2833
Location:   ubuntu-VirtualBox->/var/log/syslog
  Sep 22 10:56:32 ubuntu-VirtualBox crontab[3155]: (root) REPLACE (root)

Level:      8 - Information from the user was changed                             2020 Sep 22 10:54:37
Rule Id:    5904
Location:   ubuntu-VirtualBox->/var/log/auth.log
  Sep 22 10:54:36 ubuntu-VirtualBox chfn[3045]: changed user 'darklord' information

Level:      8 - New user added to the system                                      2020 Sep 22 10:54:29
Rule Id:    5902
Location:   ubuntu-VirtualBox->/var/log/auth.log
  Sep 22 10:54:28 ubuntu-VirtualBox useradd[2971]: new user: name=darklord, UID=1001, GID=1001, home=/home/darklord, shell=/bin/bash

Level:      15 - Attacks followed by the addition of an user.                     2020 Sep 22 10:54:29
Rule Id:    40501
Location:   ubuntu-VirtualBox->/var/log/auth.log
  Sep 22 10:54:28 ubuntu-VirtualBox groupadd[2967]: new group: name=darklord, GID=1001
  Sep 22 10:53:57 ubuntu-VirtualBox sshd[2843]: Accepted password for ubuntu from 192.168.56.1 port 58331 ssh2
  Sep 22 10:53:57 ubuntu-VirtualBox sshd[2843]: Accepted password for ubuntu from 192.168.56.1 port 58331 ssh2

Level:      12 - Multiple authentication failures followed by a success.          2020 Sep 22 10:53:57
Rule Id:    40112
Location:   ubuntu-VirtualBox->/var/log/auth.log
Src IP:     192.168.56.1
User:       ubuntu
  Sep 22 10:53:57 ubuntu-VirtualBox sshd[2843]: Accepted password for ubuntu from 192.168.56.1 port 58331 ssh2
```

Threat Mitigation

- **Mitigation Measures**

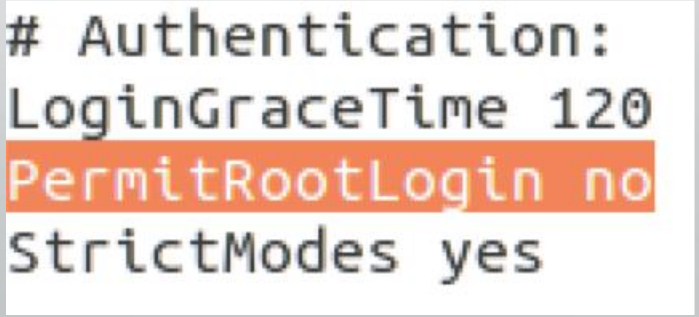
- A new IP table rules is created to block all the incoming requests from the attacker IP (192.168.56.1).



```
ubuntu@ubuntu-VirtualBox:~$ sudo iptables -A INPUT -s 192.168.56.1 -j DROP
[sudo] password for ubuntu:
ubuntu@ubuntu-VirtualBox:~$
```

- The SSH is configured to deny the root login through it.

etc/ssh/sshd.config



```
# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
```

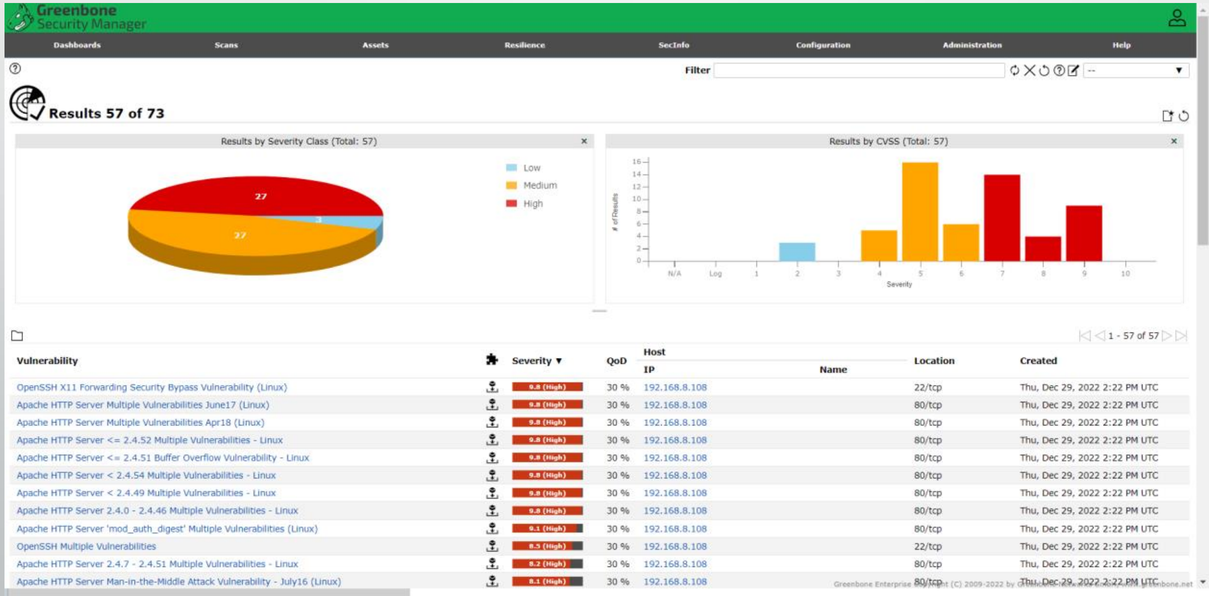
Threat Mitigation

- **Additional Recommended Measures.**
- Configure second factor authentication.
- Change the default SSH options such as:
  - Disable root login.
  - Change default port.
  - Use "AllowUsers" to restrict users access.
- Restrict the number of failed login attempts.

Hardening

- **Apache Server**

A scan using OpenVAS vulnerability scanner is conducted to identify the weaknesses on the server. It is clear from the result; that the server was misconfigured and can be exploited by an attacks in the future.



Results 57 of 73

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)	9.8 (High)	30 %	192.168.8.108		22/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server Multiple Vulnerabilities June17 (Linux)	9.8 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux)	9.8 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux	9.8 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux	9.8 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux	9.8 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux	9.8 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux	9.8 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux)	9.1 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC
OpenSSH Multiple Vulnerabilities	8.5 (High)	30 %	192.168.8.108		22/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Linux	8.2 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC
Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux)	8.1 (High)	30 %	192.168.8.108		80/tcp	Thu, Dec 29, 2022 2:22 PM UTC

Greenbone Enterprise Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

Hardening

- **Patching Apache**

- The Apache version and the OS information have been removed to not be a publicly visible. In order to make it harder for the attacker to perform attacks on the server.

Hardening

- **Privileges**

- A new Apache user and group have been created in order to make the Apache server runs as low privileged user.