Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Somayeh Izad, Ireedui Batsaikhan, Mukhlissa Khojayeva,
Ardan Goin, Alissa Perri, Mark Hurley

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

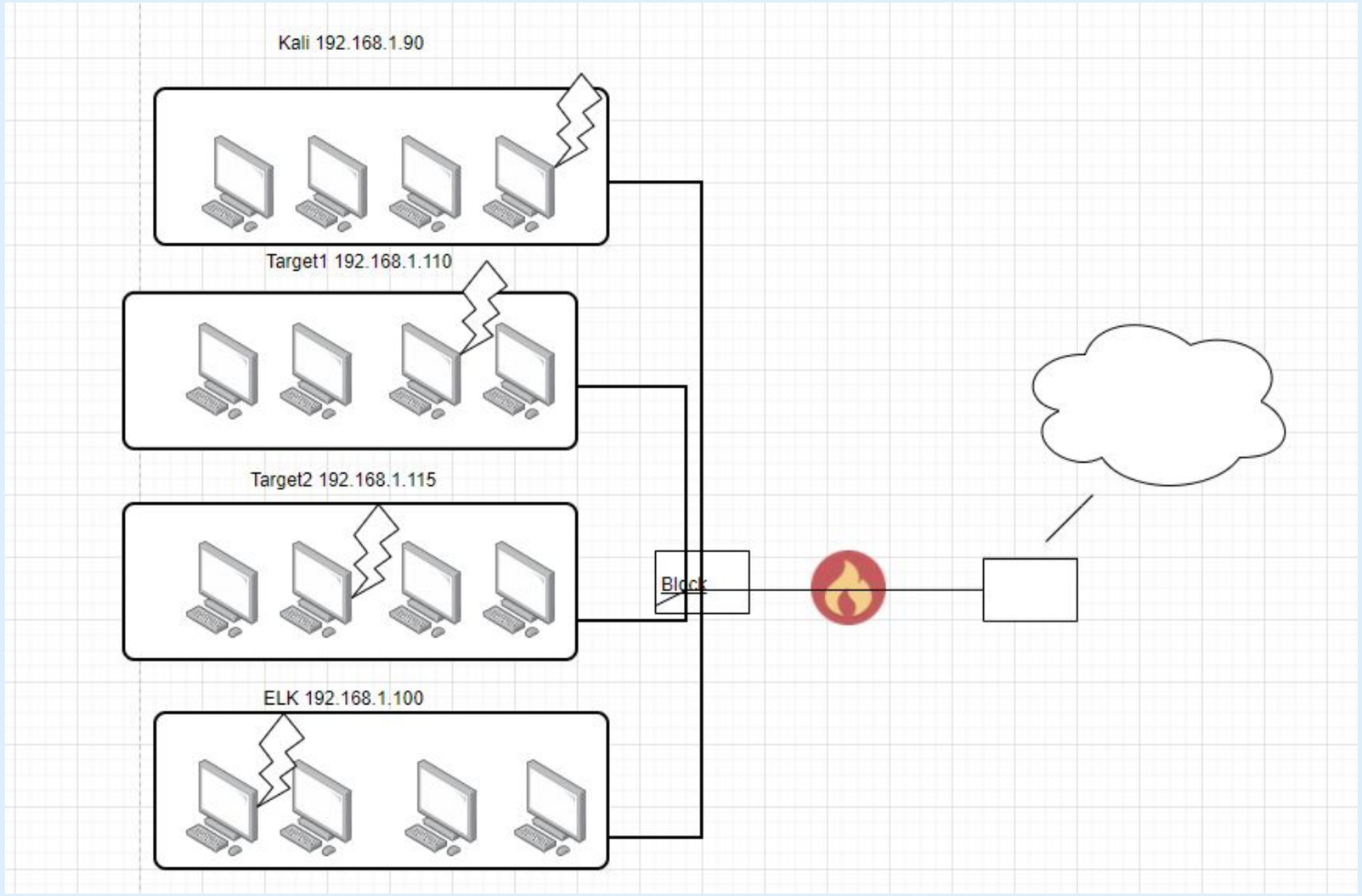
Exploits Used

Avoiding Detect

Maintaining Access

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0=24
Gateway: 192.168.1.1

Machines
IPv4:192.168.1.100
OS: Unbutu
Hostname: ELK

IPv4: 192.168.1.110
OS: Unbutu
Hostname: Target 1

IPv4:192.168.1.90
OS: Unbutu
Hostname: Kali

IPv4: 192.168.1.115
OS: Unbutu
Hostname: Target 2

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak Password Policy	Password strength is the measure of effectiveness a password resists guessing and brute force attacks.	Weak passwords are an easy target for brute force attacks which will lead to compromise system security.
Privilege Escalation Vulnerability	Able to escalate sudo privileges for user Steven	With escalated privileges one is able to gain access to more systems and spread throughout the network
SSH	22/TCP	Open SSH
HTTP	80/TCP	Apache http 2.4.10

Exploits Used

Exploitation: [SSH]

Summarize the following:

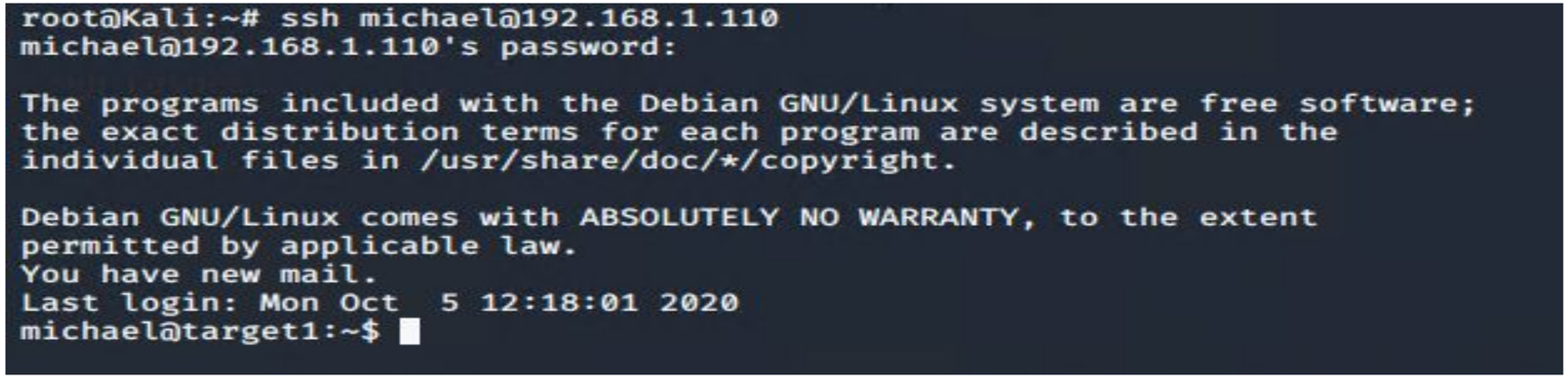
- How did you exploit the vulnerability? E.g., which tool (Nmap, etc.) or technique (XSS, etc.)?

Weak password requirements allowed to SSH in as Michael

- What did the exploit achieve? E.g., did it grant you a user shell, root access, etc.?

Gaining user access and to their shell

- Include a screenshot or command output illustrating the exploit.



Exploitation: [HTTP]

Summarize the following:

- How did you exploit the vulnerability? E.g., which tool (Nmap, etc.) or technique (XSS, etc.)?

Nmap and wpscan

- What did the exploit achieve? E.g., did it grant you a user shell, root access, etc.?

Enumerating users and vulnerabilities plugins from wordpress website

- Include a screenshot or command output illustrating the exploit.

wpscan --url http://192.168.1.110/wordpress --wp-content-dir-eu

Exploitation: [MySQL 5.5]

Summarize the following:

- How did you exploit the vulnerability? E.g., which tool (Nmap, etc.) or technique (XSS, etc.)?

Hosting the file with Python’s SimpleHTTPServer module

- What did the exploit achieve? E.g., did it grant you a user shell, root access, etc.?

Log in to the MySQL database mysql

- Include a screenshot or command output illustrating the exploit.

python -m SimpleHTTPServer 80

Avoiding Detection

Stealth Exploitation of [HTTP Errors]

Monitoring Overview

- Which alerts detect this exploit? Excessive HTTP Errors
- Which metrics do they measure? http.response.status_code
- Which thresholds do they fire at? 400

Mitigating Detection

- How can you execute the same exploit without triggering the alert?

  if we have possession of the Hash password, you can brute force them offsite.
- Are there alternative exploits that may perform better?

  It is possible to use phishing in conjunction with metasploit to target the users

Stealth Exploitation of [HTTP Request Size]

Monitoring Overview

- Which alerts detect this exploit? HTTP Request Size Monitor
- Which metrics do they measure? sum of http request bytes
- Which thresholds do they fire at? 3500

Mitigating Detection

- How can you execute the same exploit without triggering the alert?

  by keeping cookies and request headers as small as possible to ensure that it will fit in a single packet.
- Are there alternative exploits that may perform better?

  By using scp to extract or upload files

Stealth Exploitation of [CPU Usage Monitor]

Monitoring Overview

- Which alerts detect this exploit? CPU Usage Monitor
- Which metrics do they measure? max of system process cpu total pct
- Which thresholds do they fire at? 0.5 pct

Mitigating Detection

- How can you execute the same exploit without triggering the alert?

- Are there alternative exploits that may perform better?
- If possible, include a screenshot of your stealth technique.

Maintaining Access

Backdooring the Target

Backdoor Overview

- What kind of backdoor did you install (reverse shell, shadow user, etc.)?

  Reverse shell/backdoor.php with netcat listener

- How did you drop it (via Metasploit, phishing, etc.)?

  by using an Ncat connection to run a script that would upload the file.

  Command= ncat 192.168.1.115 80

- How do you connect to it?

  http://192.168.1.115/contact.php?cmd=id

[Network Topology & Critical Vulnerabilities]

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

Alerts Implemented

Hardening

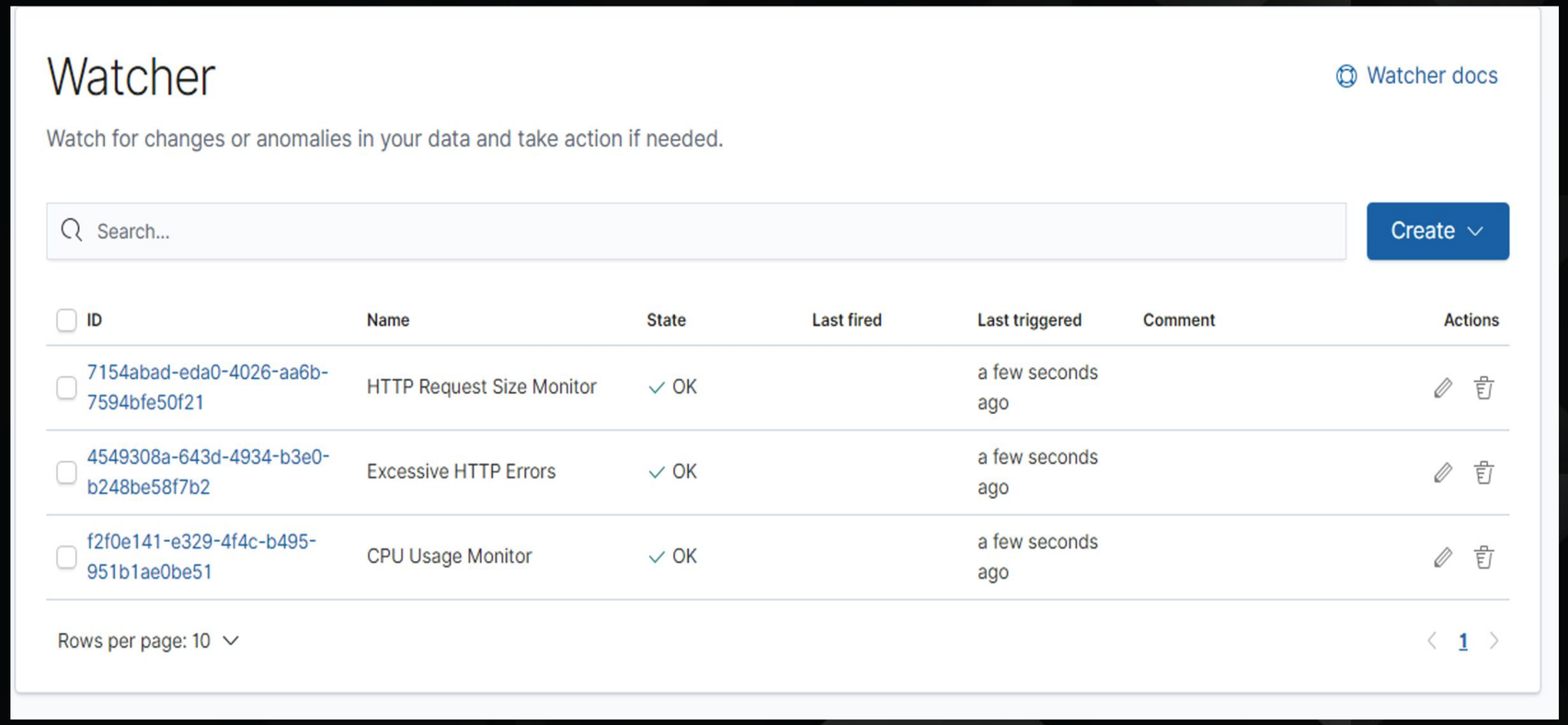
Implementing Patches

Critical Vulnerabilities: Target 1

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

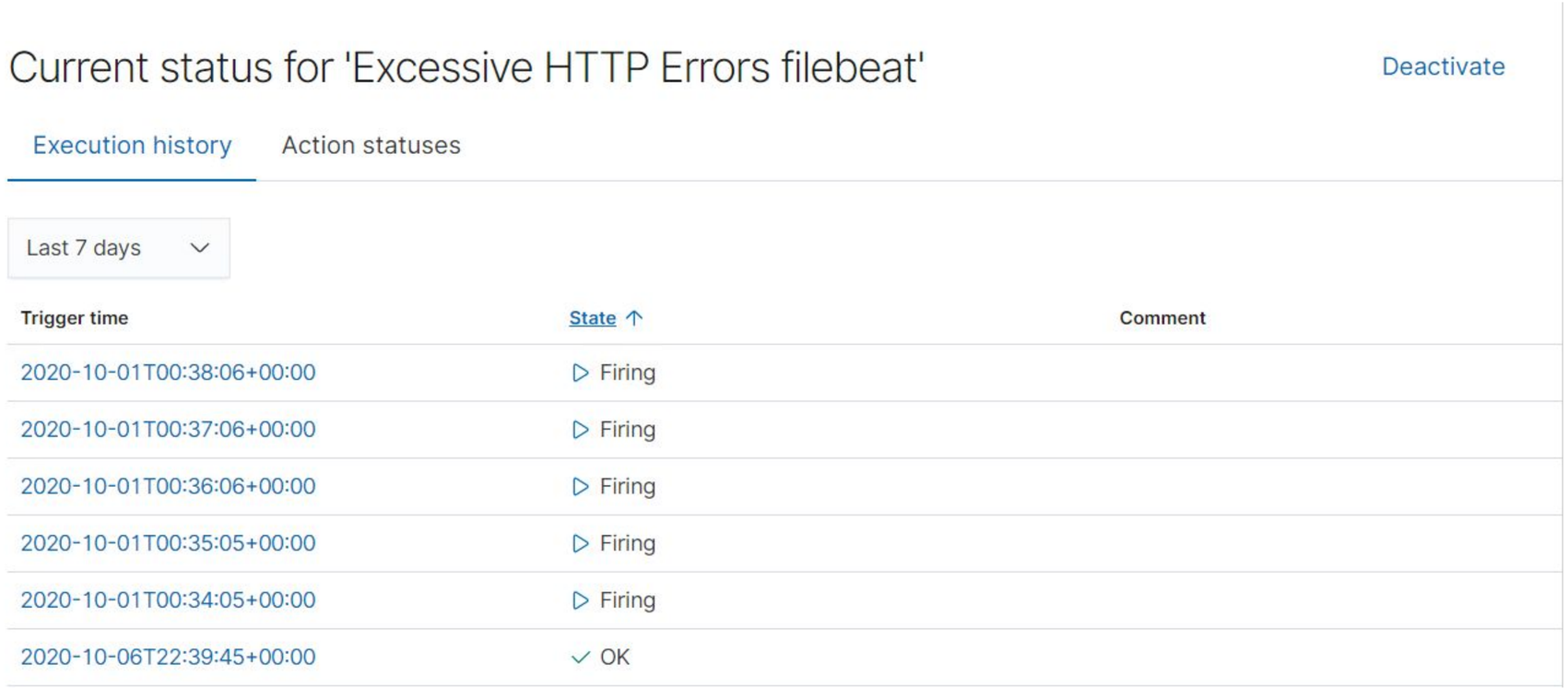
Vulnerability	Description	Impact
SSH	22/TCP Open SSH	Medium
HTTP	80/TCP Apache httpd 2.4.10	High
rpcbind	111/TCP 2-4	Medium
netbios-ssn	139/TCP Samba smbd 3.X-4.X	Medium

Alerts Implemented



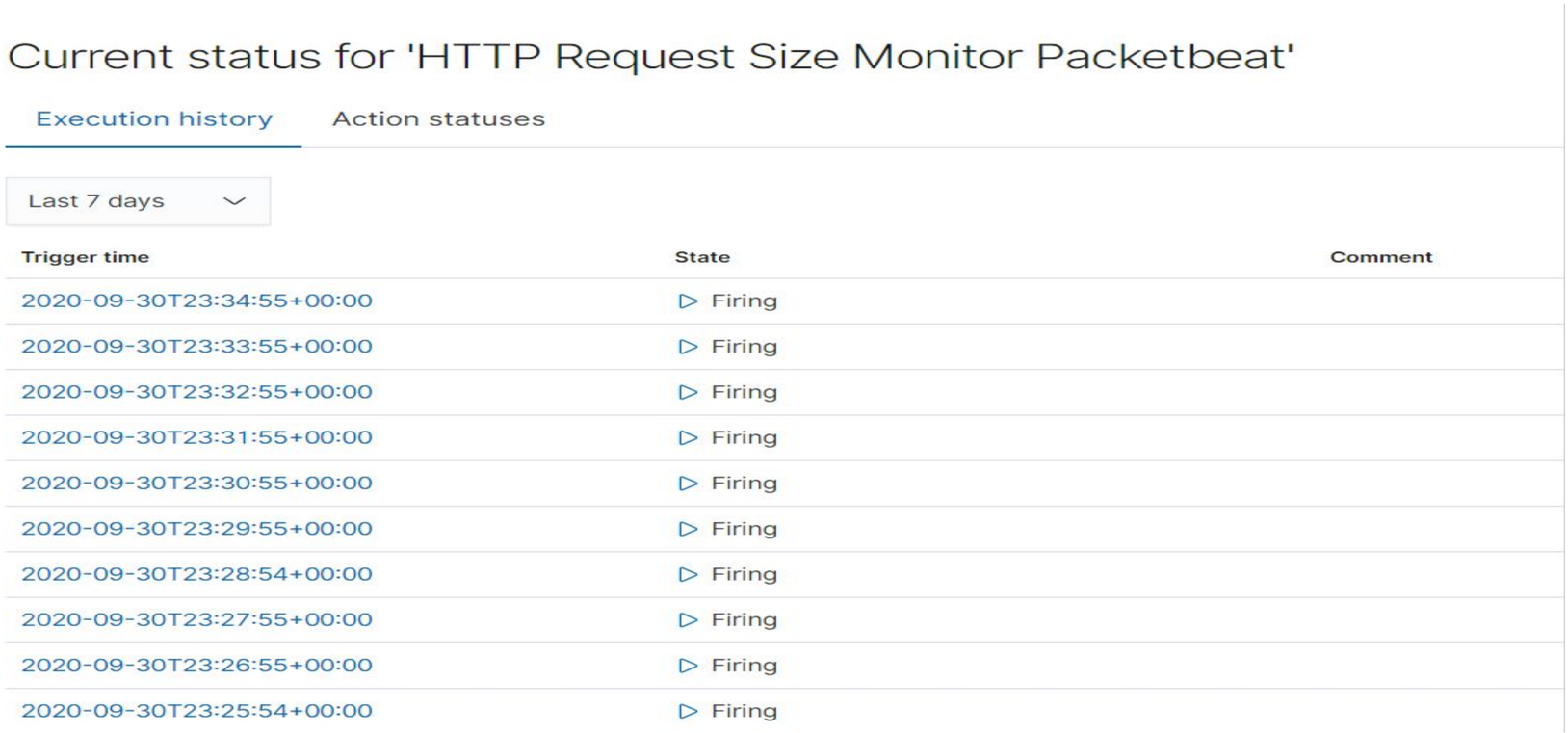
[Excessive HTTP Errors]

- Monitors the HTTP errors using filebeat
- The **threshold** is above 400 for the last 5 mins
- Helps to mitigate Brute Force Attacks



[HTTP Request Size Monitor]

- Monitors http.request.bytes using filebeat and packetbeat
- The threshold is above 3500 for the last minute
- Helps to mitigate Denial of Service Attacks



[CPU Usage Monitor]

- Monitors the system.process.cpu.total.pct using metricbeat
- Threshold is above 0.5 for the last 5 minutes
- Helps to mitigate the Excessive CPU usage
- The Alert did not run (Most likely, it didn’t exceed the threshold)

Hardening

Hardening Against Weak Password Requirements on Target 1

- Patch:
  - Require stronger passwords.
    - Include upper and lowercase letters, symbols and numbers. Paswrods shoud be greater than 12 characters and should be changed every 60-90 days
  - Implement 2 factor authentication
- Why It Works:
  - Stronger passwords will be more difficult to crack by hackers
  - 2 factor authentication provides a second line of authentication

Hardening Against Apache/2.4.10 (Debian) CVE-2019-10098 on Target 1

- Patch:
  - **Patch** oval:com.redhat.rhsa:def:20203958
- Why It Works:
  - The patch fixes CVE-2019-10098. httpd: mod_rewrite potential open redirect (CVE-2019-10098). It stops the possibility of rewriting, changing and redirecting the URL.

Hardening Against Rpcbind CVE-2017-8779 on Target 1

- Patch:
  - **Patch** oval:com.redhat.rhsa:def:2017126

- Why It Works:
  - It fixes the way rpcbind uses libtirpc (libntirpc), a memory leak can occur when parsing specially crafted XDR messages. An attacker sending thousands of messages to rpcbind could cause its memory usage to grow without bound, eventually causing it to be terminated by the OOM killer. (CVE-2017-8779)

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

Ansible is a popular open-source tool that provides automation, configuration management, and orchestration all in one. The patching is customizable via role’s variables definition.

Run:

ansible-playbook orapatch.yml -k

The -k option will prompt you to enter the SSH password.

if you are using SSH keys then -k option dont have to be used.

[Start of Network Analysis]

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205(26m Bytes) 166.62.111.64(16m Bytes)	Machines that sent the most traffic.
Most Common Protocols	UDP TCP TLSv.1.2 and 1.3	Three most common protocols on the network.
# of Unique IP Addresses	808	Count of observed IP addresses.
Subnets	255.255.255.0 is the only range observed in the private ip’s	Observed subnet ranges.
# of Malware Species	68	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

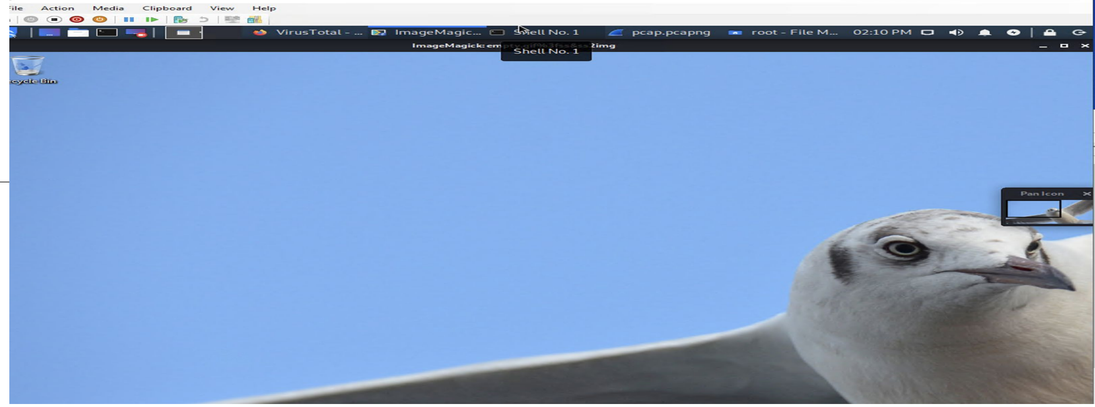
- Downloading and installing desktop backgrounds

Suspicious Activity

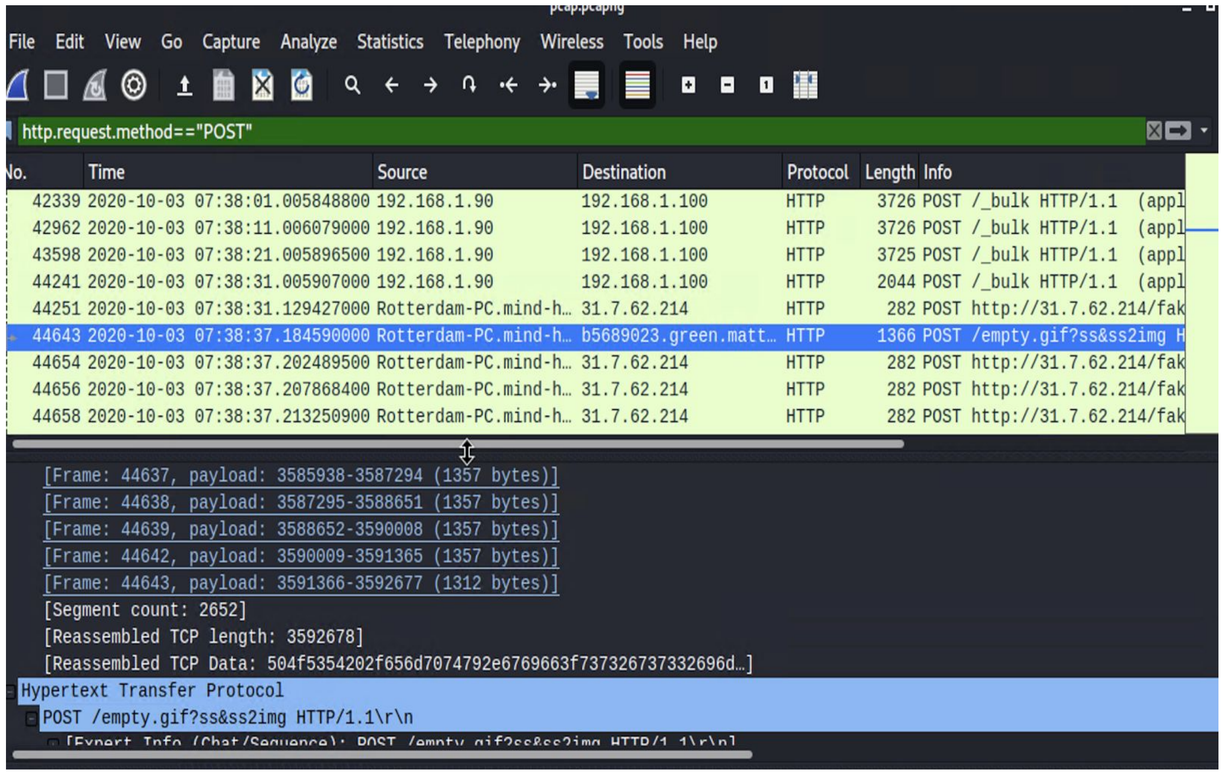
- Set up AD network and domain controller
- Downloading malware

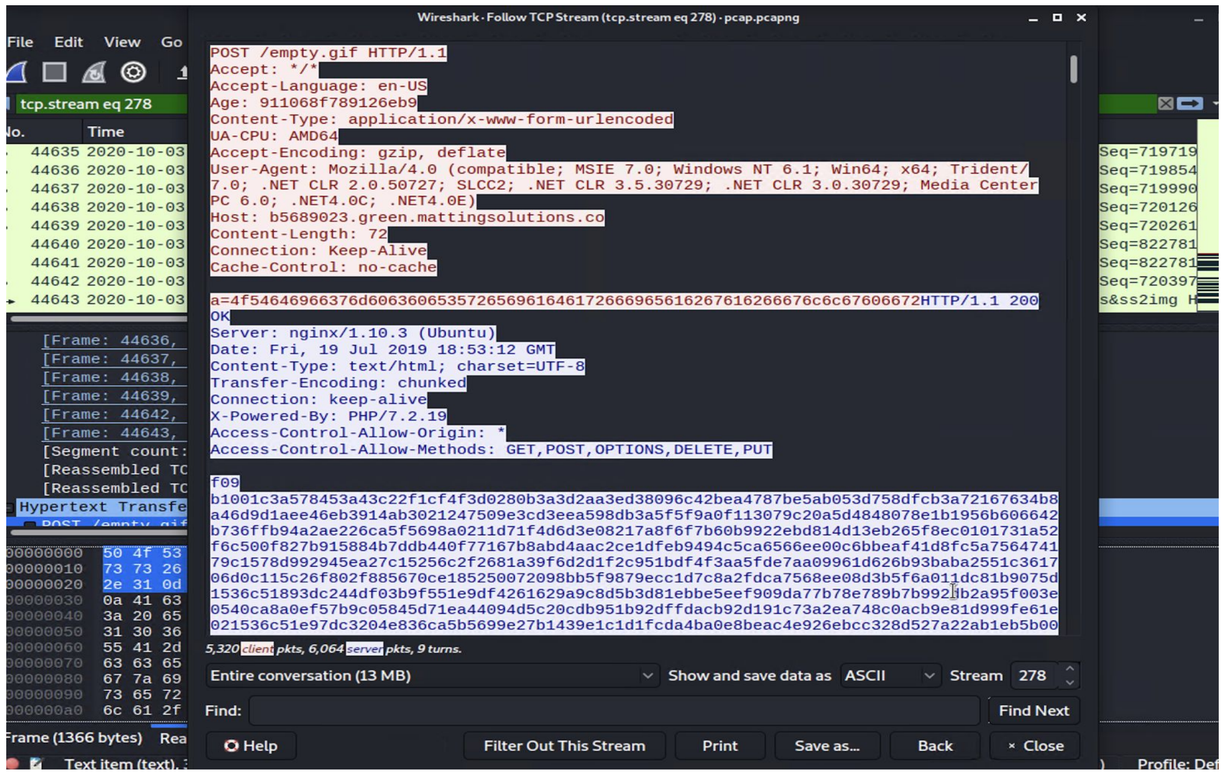
Normal and Malicious Activity

[Installing Desktop Backgrounds]



- What kind of traffic did you observe? HTTP Protocol, POST
- What, specifically, was the user doing? Which site were they browsing? Etc.Installing Desktop Background. b5689023.green.mattingsolutions.co





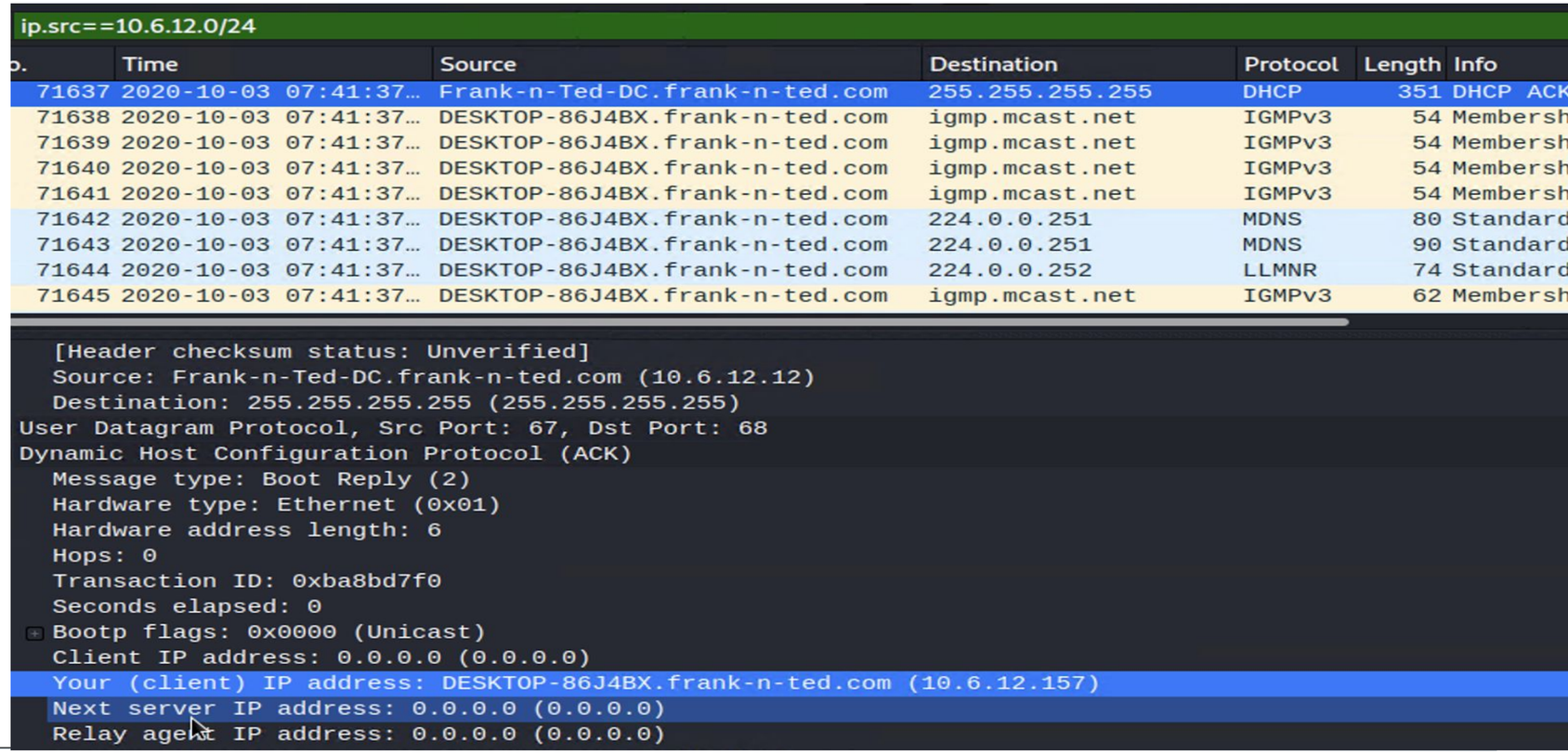
[Set up AD Network and Domain Controller]

- What kind of traffic did you observe? Which protocol(s)?

  We observed the client traffic and the server traffic which included DHCP, TCP ,DNS, HTTP,LDAP protocols.The user was getting authentication for the Frank-n-ted.com domain.

- Domain name: Frank-n-Ted-DC.frank-n-ted.com and User: DESKTOP-86J4BX.frank-n-ted.com - subnet mask: 255.255.255.0

  Domain Controller (DC) of the AD Network is 10.6.12.12



[Downloading Malware]

- What kind of traffic did you observe? Which protocol(s)?

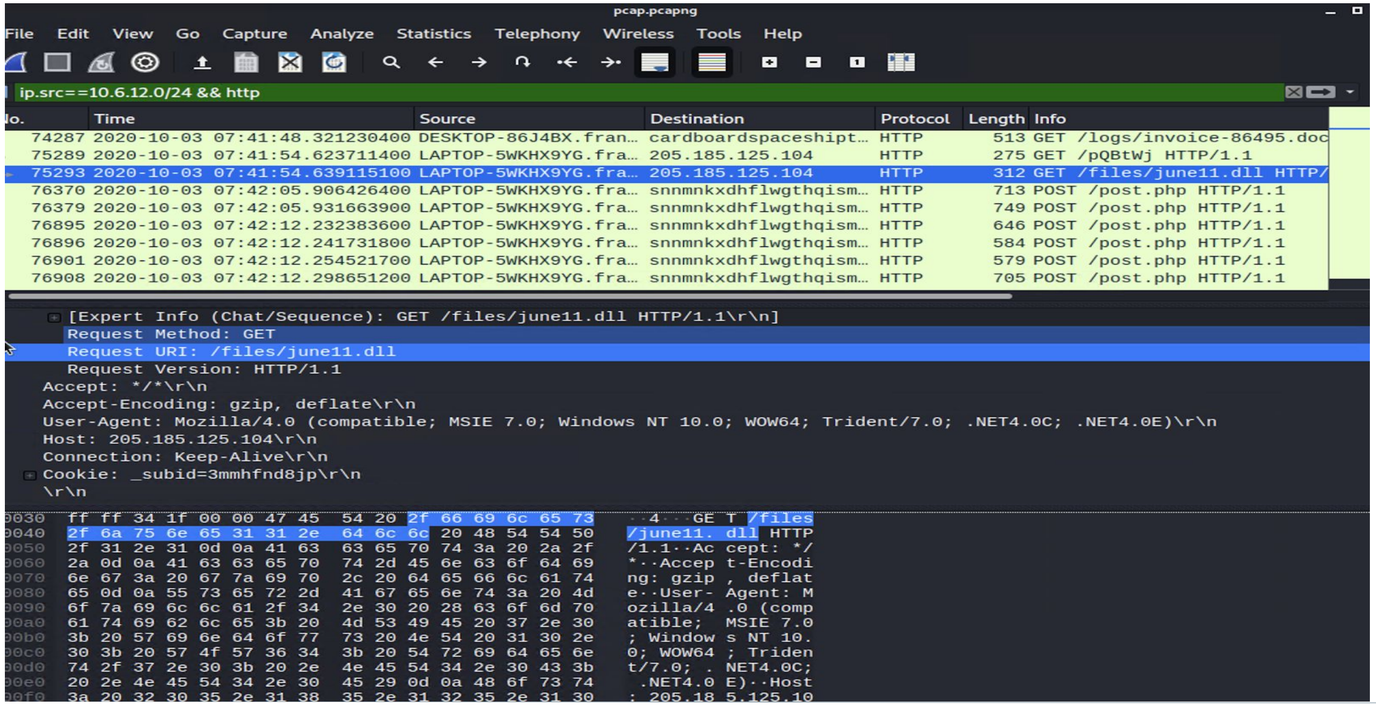
  We observed the HTTP traffic being downloaded and there was malicious traffic.

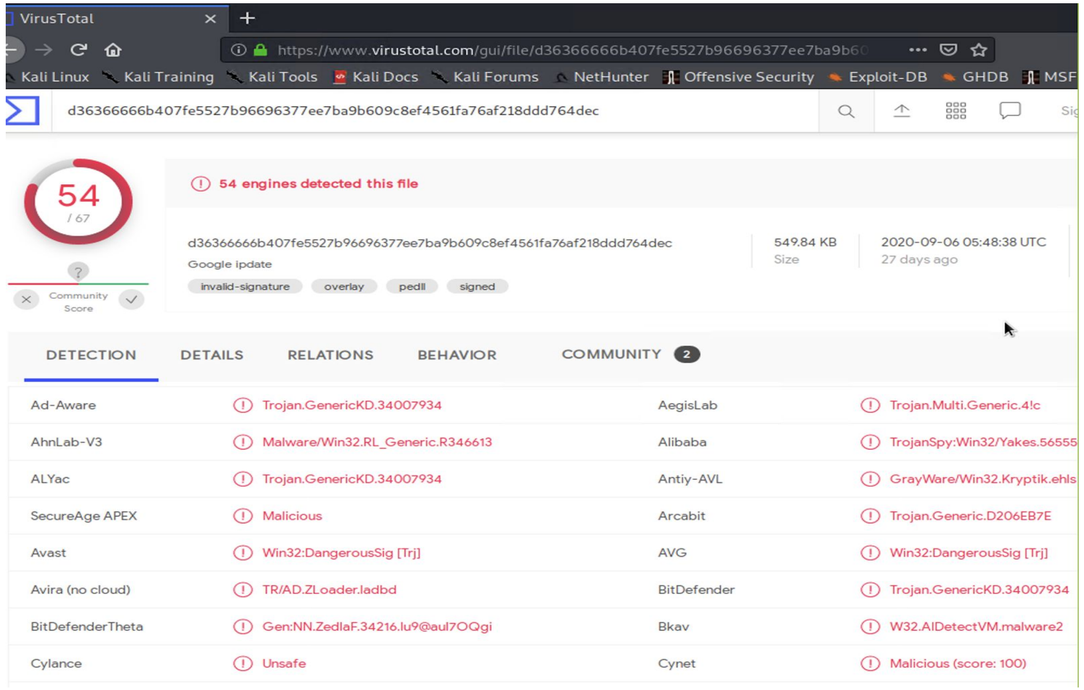
- What, specifically, was the user doing? Which site were they browsing? Etc.

  The user downloaded malware. Host: http://205.185.125.104/files/june11.dll

- Include a description of any interesting files.

  The file contained malware binaries, including trojan.





The End