Final Engagement

Network Analysis of a Vulnerable Network

Team Animal Farm

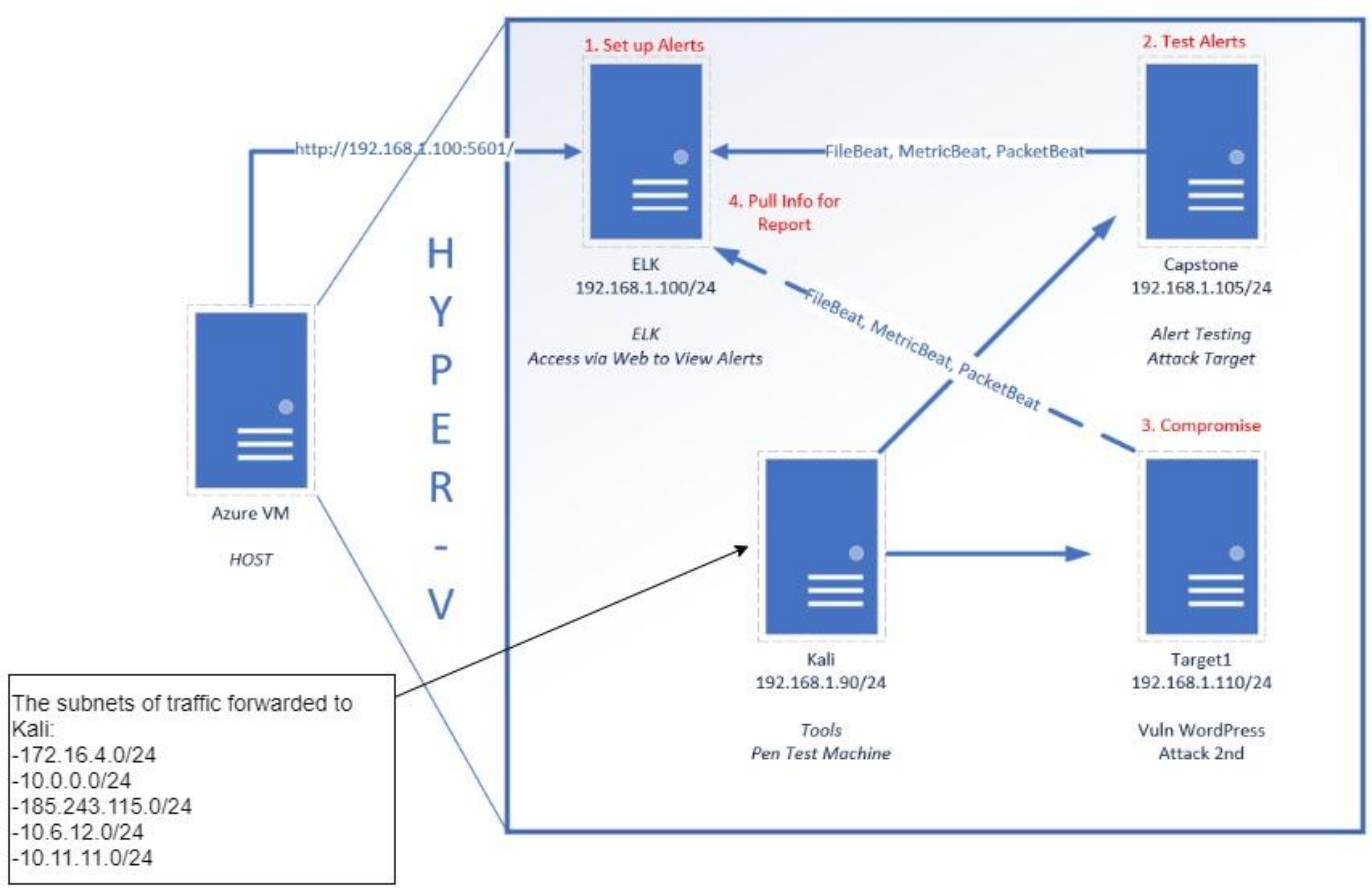
Tomoro Carpender, James O’Connor, Justin Paquin,
Ashley Hart, Andrew Stone, and Jon Klothe

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

Network Topology



The subnets of traffic forwarded to Kali:
-172.16.4.0/24
-10.0.0.0/24
-185.243.115.0/24
-10.6.12.0/24
-10.11.11.0/24

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

Machines
IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

IPv4: 192.168.1.110
OS: Linux 3.2 - 5.9
Hostname: Target 1

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

Critical Vulnerabilities: Internal Network

Our assessment uncovered the following critical vulnerabilities in **Internal Network**

Vulnerability	Description	Impact
Unauthorized Web Server	Employees had a unauthorized Web Server on the company network	This opens up the network to a huge amount of risk. OWASP list item such as Code Injects, Broken Authentication Cross-site scripting and many more issues to running even authorized web server.
Trojan Virus Download	File june11.d11 was downloaded and has a trojan virus	This file infected the victims machine and most like would have infected the entire network
Illegal Download	An Torrent file was downloaded which was -Betty_Boop_on_the_Rhthym_on_the Reservation.avi.torrent	Users could download Malware which could lead to issues with Data Safety as well as possible Legal Issues. The Legal issues stems from the unauthorized copyrighted items being shared on the company network.

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers 5 (IP Addresses)	172.16.4.205, 10.0.0.201, 185.243.115.84, 10.6.12.203, 10.11.11.200	Machines that sent the most traffic.
Most Common Protocols	TCP UDP	Three most common protocols on the network.
# of Unique IP Addresses	108400	Count of observed IP addresses.
Subnets	172.16.4.0/24, 10.0.0.0/24, 185.243.115.0/24, 10.6.12.0/24, 10.11.11.0/24	Observed subnet ranges.
# of Malware Species	june11.dll	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

- Site Browsing:
    - Chromebooktrivia
    - Youtube
    - Blogging
    - Reading news
    - Hobby websites

Suspicious Activity

- Downloading and sending malware
- Torrenting
- Phishing

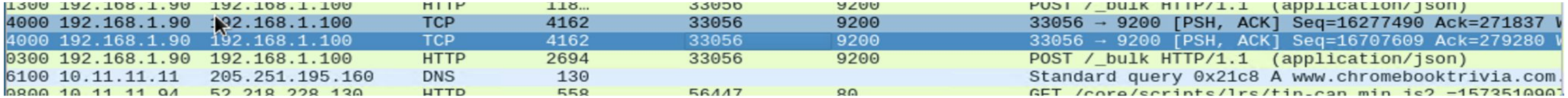
Normal Activity

Web Browsing Traffic Analysis

Summary of traffic:

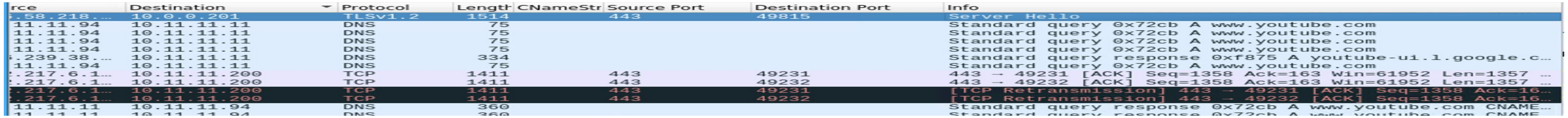
- The following protocols were observed with the following actions:
  - Web based traffic using the HTTP Protocol
- What were the most common sites visited and for what purpose:
  - Orbike.com, Chromebook Trivia, and You.tube
    - Playing Trivia
    - Researching Cycling including riding and events
    - Watching videos

Trivia:



```
1300 192.168.1.90  192.168.1.100   HTTP  118…  33056  9200  POST /_bulk HTTP/1.1  (application/json)
4000 192.168.1.90  192.168.1.100   TCP   4162  33056  9200  33056 → 9200 [PSH, ACK] Seq=16277490 Ack=271837 W
4000 192.168.1.90  192.168.1.100   TCP   4162  33056  9200  33056 → 9200 [PSH, ACK] Seq=16707609 Ack=279280 W
0300 192.168.1.90  192.168.1.100   HTTP  2694  33056  9200  POST /_bulk HTTP/1.1  (application/json)
6100 10.11.11.11   205.251.195.160 DNS    130               Standard query 0x21c8 A www.chromebooktrivia.com.
0800 10.11.11.94   52.218.228.130  HTTP   558  56447    80  GET /core/scripts/lrs/tin-can.min.js?_=157351090
```

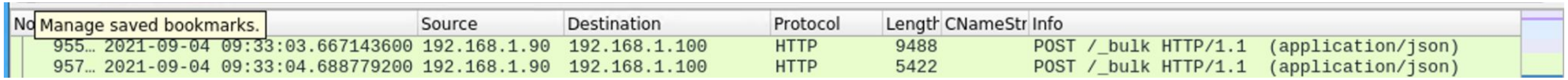
Youtube:



```
rce           Destination      Protocol  Length CNameStr Source Port  Destination Port  Info
.58.218.…     10.0.0.201       TLSv1.2   1514            443          49815             Server Hello
11.11.94      10.11.11.11      DNS         75                                           Standard query 0x72cb A www.youtube.com
11.11.94      10.11.11.11      DNS         75                                           Standard query 0x72cb A www.youtube.com
11.11.94      10.11.11.11      DNS         75                                           Standard query 0x72cb A www.youtube.com
11.11.94      10.11.11.11      DNS         75                                           Standard query 0x72cb A www.youtube.com
.239.38.…     10.11.11.11      DNS        334                                           Standard query response 0xf875 A youtube-ui.l.google.c…
11.11.94      10.11.11.11      DNS         75                                           Standard query 0x72cb A www.youtube.com
.217.6.1…     10.11.11.200     TCP       1411            443          49231             443 → 49231 [ACK] Seq=1358 Ack=163 Win=61952 Len=1357 …
.217.6.1…     10.11.11.200     TCP       1411            443          49232             443 → 49232 [ACK] Seq=1358 Ack=163 Win=61952 Len=1357 …
.217.6.1…     10.11.11.200     TCP       1411            443          49231             [TCP Retransmission] 443 → 49231 [ACK] Seq=1358 Ack=16…
.217.6.1…     10.11.11.200     TCP       1411            443          49232             [TCP Retransmission] 443 → 49232 [ACK] Seq=1358 Ack=16…
11.11.11      10.11.11.94      DNS        360                                           Standard query response 0x72cb A www.youtube.com CNAME…
11.11.11      10.11.11.94      DNS        360                                           Standard query response 0x72cb A www.youtube.com CNAME
```

Conclusion of this traffic is that these activities were fairly consistent traffic and would be detrimental to productivity. Recommendation of managing web traffic would be to install a content filter on network devices.

Normal good file traffic was that we noticed JSON has php files and found this traffic our Kibana monitoring for our network :



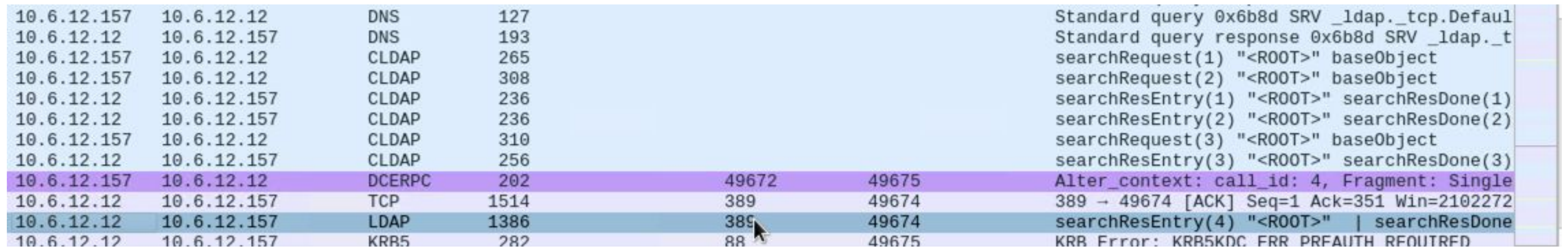
```
No Manage saved bookmarks.           Source        Destination    Protocol  Length CNameStr Info
  955… 2021-09-04 09:33:03.667143600 192.168.1.90  192.168.1.100  HTTP      9488            POST /_bulk HTTP/1.1  (application/json)
  957… 2021-09-04 09:33:04.688779200 192.168.1.90  192.168.1.100  HTTP      5422            POST /_bulk HTTP/1.1  (application/json)
```

Malicious Activity

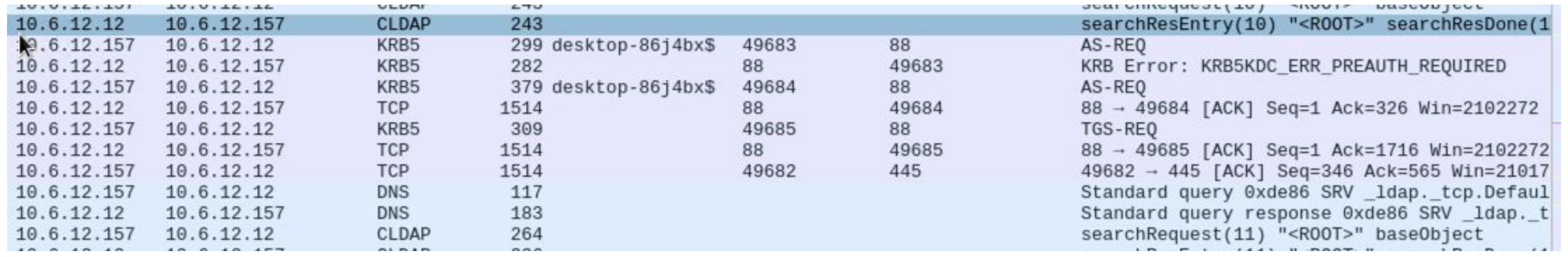
Hosting of an Unauthorized Web Server

Summarizing the following

- What kind of traffic did you observe? Which protocol(s)?
    - ■ There are many requests to change or find information in directories using LDAP and CLDAP
        - We see TCP, CLDAP, LDAP, DNS, and HTTP
    - ■ What, specifically, was the user doing? Which site were they browsing?
        - ○ The traffic seems to be doing quite a few LDAP and CLDAP
        - ○ In research the traffic this looks like request to search and updated directories and I also see the requests are being done as root.



```
10.6.12.157  10.6.12.12   DNS     127                  Standard query 0x6b8d SRV _ldap._tcp.Defaul
10.6.12.12   10.6.12.157  DNS     193                  Standard query response 0x6b8d SRV _ldap._t
10.6.12.157  10.6.12.12   CLDAP   265                  searchRequest(1) "<ROOT>" baseObject
10.6.12.157  10.6.12.12   CLDAP   308                  searchRequest(2) "<ROOT>" baseObject
10.6.12.12   10.6.12.157  CLDAP   236                  searchResEntry(1) "<ROOT>" searchResDone(1)
10.6.12.12   10.6.12.157  CLDAP   236                  searchResEntry(2) "<ROOT>" searchResDone(2)
10.6.12.157  10.6.12.12   CLDAP   310                  searchRequest(3) "<ROOT>" baseObject
10.6.12.12   10.6.12.157  CLDAP   256                  searchResEntry(3) "<ROOT>" searchResDone(3)
10.6.12.157  10.6.12.12   DCERPC  202   49672   49675  Alter_context: call_id: 4, Fragment: Single
10.6.12.12   10.6.12.157  TCP     1514  389     49674  389 → 49674 [ACK] Seq=1 Ack=351 Win=2102272
10.6.12.12   10.6.12.157  LDAP    1386  389     49674  searchResEntry(4) "<ROOT>"  | searchResDone
10.6.12.12   10.6.12.157  KRB5    282   88      49675  KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
```

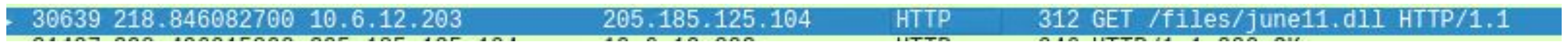


```
10.6.12.12   10.6.12.157  CLDAP   243                                  searchResEntry(10) "<ROOT>" searchResDone(1
10.6.12.157  10.6.12.12   KRB5    299 desktop-86j4bx$  49683  88      AS-REQ
10.6.12.12   10.6.12.157  KRB5    282                  88     49683   KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
10.6.12.157  10.6.12.12   KRB5    379 desktop-86j4bx$  49684  88      AS-REQ
10.6.12.12   10.6.12.157  TCP    1514                  88     49684   88 → 49684 [ACK] Seq=1 Ack=326 Win=2102272
10.6.12.157  10.6.12.12   KRB5    309                  49685  88      TGS-REQ
10.6.12.12   10.6.12.157  TCP    1514                  88     49685   88 → 49685 [ACK] Seq=1 Ack=1716 Win=2102272
10.6.12.157  10.6.12.12   TCP    1514                  49682  445     49682 → 445 [ACK] Seq=346 Ack=565 Win=21017
10.6.12.157  10.6.12.12   DNS     117                                  Standard query 0xde86 SRV _ldap._tcp.Defaul
10.6.12.12   10.6.12.157  DNS     183                                  Standard query response 0xde86 SRV _ldap._t
10.6.12.157  10.6.12.12   CLDAP   264                                  searchRequest(11) "<ROOT>" baseObject
```

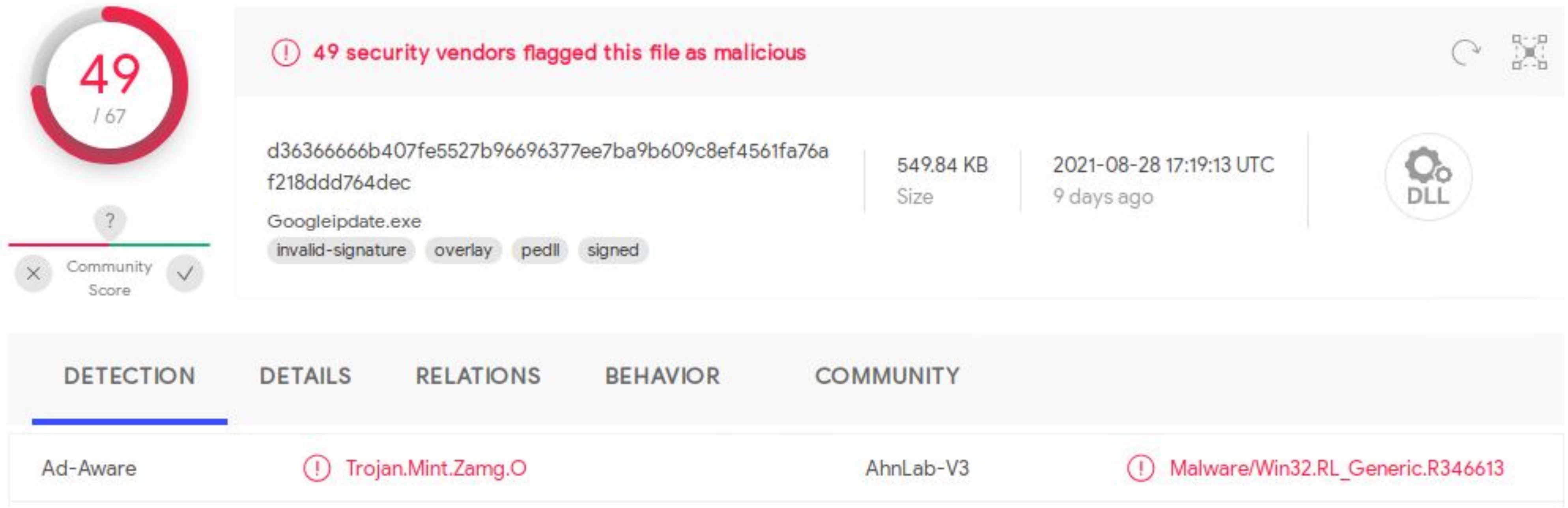
Download Malware

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - **The type of traffic that resulted in malicious behavior was from HTTP GET requests.**
- What, specifically, was the user doing? Which site were they browsing?
  - **User frank.brokowski of 10.6.21.203 downloaded Trojan Horse with filename of June11.dll. After navigating to http://205.185.125.104/files, the user clicked through to requesting the file containing the malware.**



```
30639 218.846082700 10.6.12.203          205.185.125.104     HTTP       312 GET /files/june11.dll HTTP/1.1
```



49 / 67

49 security vendors flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76a f218ddd764dec

Googleipdate.exe

549.84 KB Size

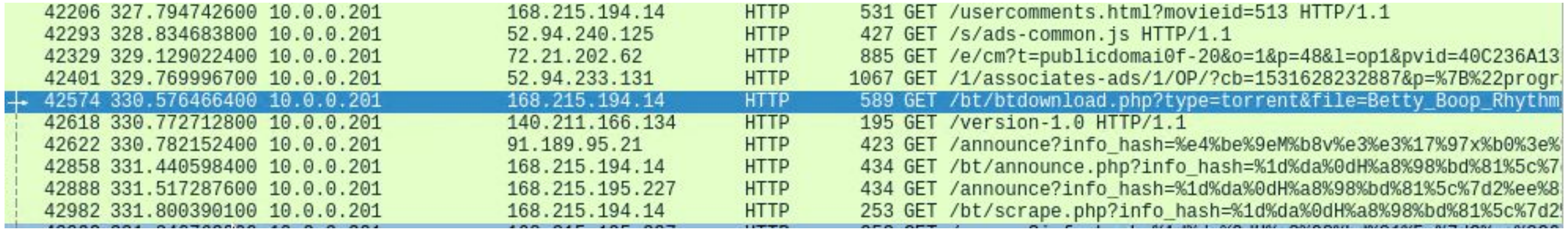
2021-08-28 17:19:13 UTC 9 days ago

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613

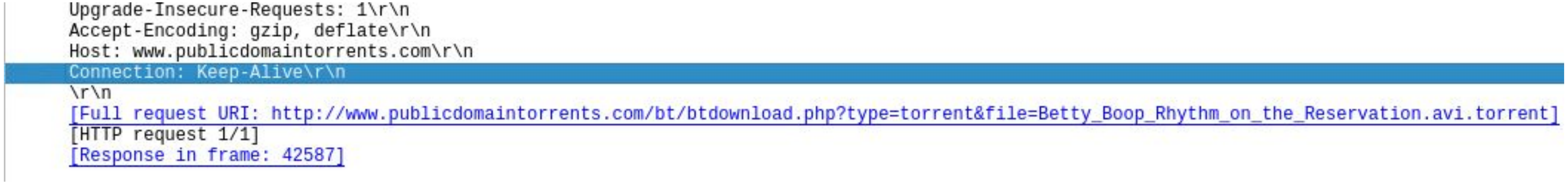
Breaking Company Policies with Illegal Downloads

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - **The type of traffic that resulted in malicious behavior was from HTTP GET request.**
- What, specifically, was the user doing? Which site were they browsing?
  - **User *blanco* broke company policy by performing an illegal download to their desktop; the torrent file downloaded was called “Betty_Boop_Rhythm_on_the_Reservation.avi.torrent”.**



```
42206 327.794742600 10.0.0.201    168.215.194.14    HTTP     531 GET /usercomments.html?movieid=513 HTTP/1.1
42293 328.834683800 10.0.0.201    52.94.240.125     HTTP     427 GET /s/ads-common.js HTTP/1.1
42329 329.129022400 10.0.0.201    72.21.202.62      HTTP     885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13
42401 329.769996700 10.0.0.201    52.94.233.131     HTTP    1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22progr
42574 330.576466400 10.0.0.201    168.215.194.14    HTTP     589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm
42618 330.772712800 10.0.0.201    140.211.166.134   HTTP     195 GET /version-1.0 HTTP/1.1
42622 330.782152400 10.0.0.201    91.189.95.21      HTTP     423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%
42858 331.440598400 10.0.0.201    168.215.194.14    HTTP     434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7
42888 331.517287600 10.0.0.201    168.215.195.227   HTTP     434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8
42982 331.800390100 10.0.0.201    168.215.194.14    HTTP     253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2
```



```
Upgrade-Insecure-Requests: 1\r\n
Accept-Encoding: gzip, deflate\r\n
Host: www.publicdomaintorrents.com\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent]
[HTTP request 1/1]
[Response in frame: 42587]
```

The End