Final Engagement

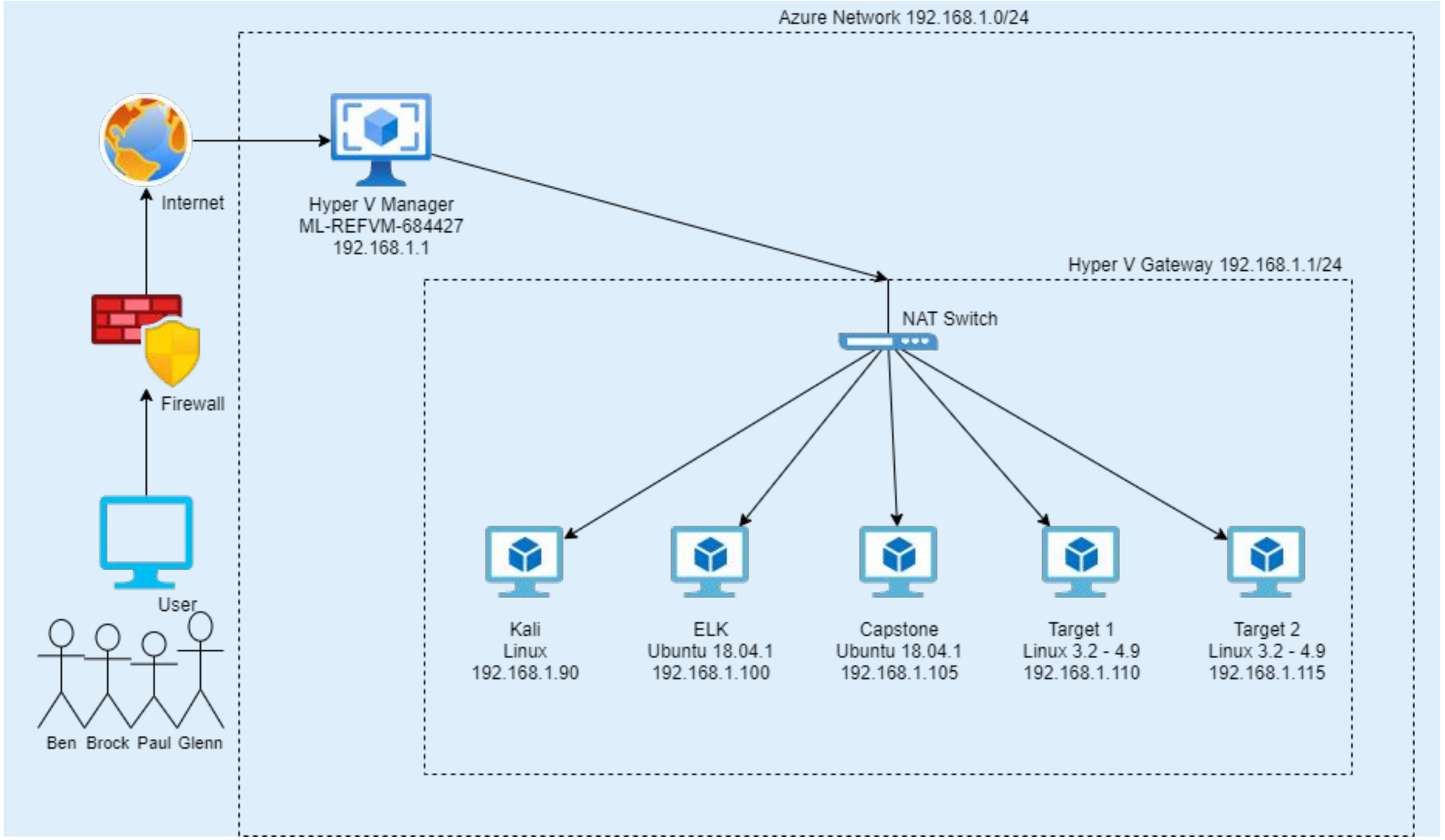
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network

Address Range: **192.168.1/24**
Netmask: **255.255.255.0**
Gateway: **192.168.1.1**

Machines

IPv4: **192.168.1.90**
OS: **Linux 2.6.32**
Hostname: **Kali**

IPv4: **192.168.1.100**
OS: **Ubuntu 18.04.01**
Hostname: **ELK**

IPv4: **192.168.1.105**
OS: **Ubuntu 18.04.01**
Hostname: **Capstone**

IPv4: **192.168.1.110**
OS: **Linux 3.2 - 4.9**
Hostname: **Target 1**

IPv4: **192.168.1.115**
OS: **Linux 3.2 - 4.9**
Hostname: **Target 2**

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Open Port Visibility	Ports were visible using Nmap.	The attacker is better able to plan their attack and tailor techniques accordingly.
WPScan Visibility	WPScan was used to show usernames for their network	The attacker was able to use these usernames to gain access to their web server.
Weak User Passwords	Multiple users had weak passwords.	The attacker was able to guess a users password to SSH into the network.
Password hashes stored in the MySQL	Hashes for users passwords were found by looking through all the databases that were available to the attacker.	The attacker was able to crack their passwords with the hashes found.
User Configuration	One of the users had Sudo privileges.	The attack was able to use sudo to escalate to a root user.

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	Ethernet · 74 | IPv4 · 877 | IPv6 · 1 | TCP · 1044 | UDP · 1839 Address A / Address B / Packets / Bytes / Packets A → B 172.16.4.205 / 185.243.115.84 / 30,344 / 26M / 15,149 166.62.111.64 / 172.16.4.205 / 15,728 / 16M / 11,354 10.0.0.201 / 23.43.62.169 / 6,934 / 7045k / 2,282 10.0.0.201 / 64.187.66.143 / 4,883 / 3637k / 2,235 5.101.51.151 / 10.6.12.203 / 4,326 / 4246k / 3,262	Machines that sent the most traffic.
Most Common Protocols	Network management protocols Network communication protocols Network security protocols	Three most common protocols on the network.
# of Unique IP Addresses	808 unique IP addresses	Count of observed IP addresses.
Subnets	10.6.12.0/24 172.16.4.0/24 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	5	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

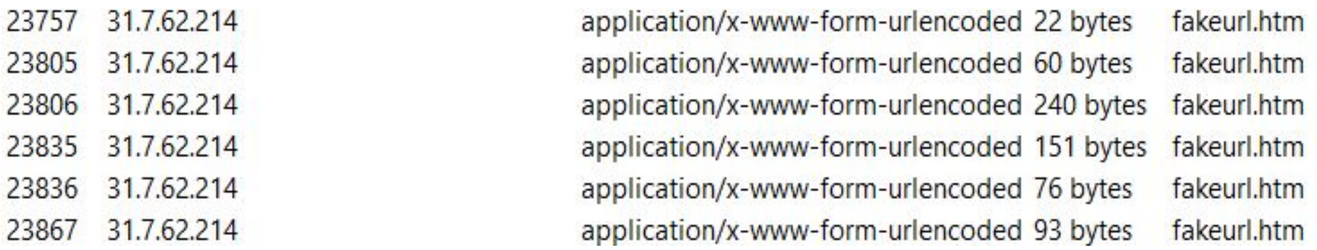
Users were observed engaging in the following kinds of activity.

“Normal” Activity

- For example: Watching YouTube, reading the news.
- assoc-amazon.om
- gooletagsrevices.com
- green mattingsolutions

Suspicious Activity

- For example: Sending malware, phishing.
- iphonehacks.com
- form-urlencoded.com
- mysocalledchoas.com

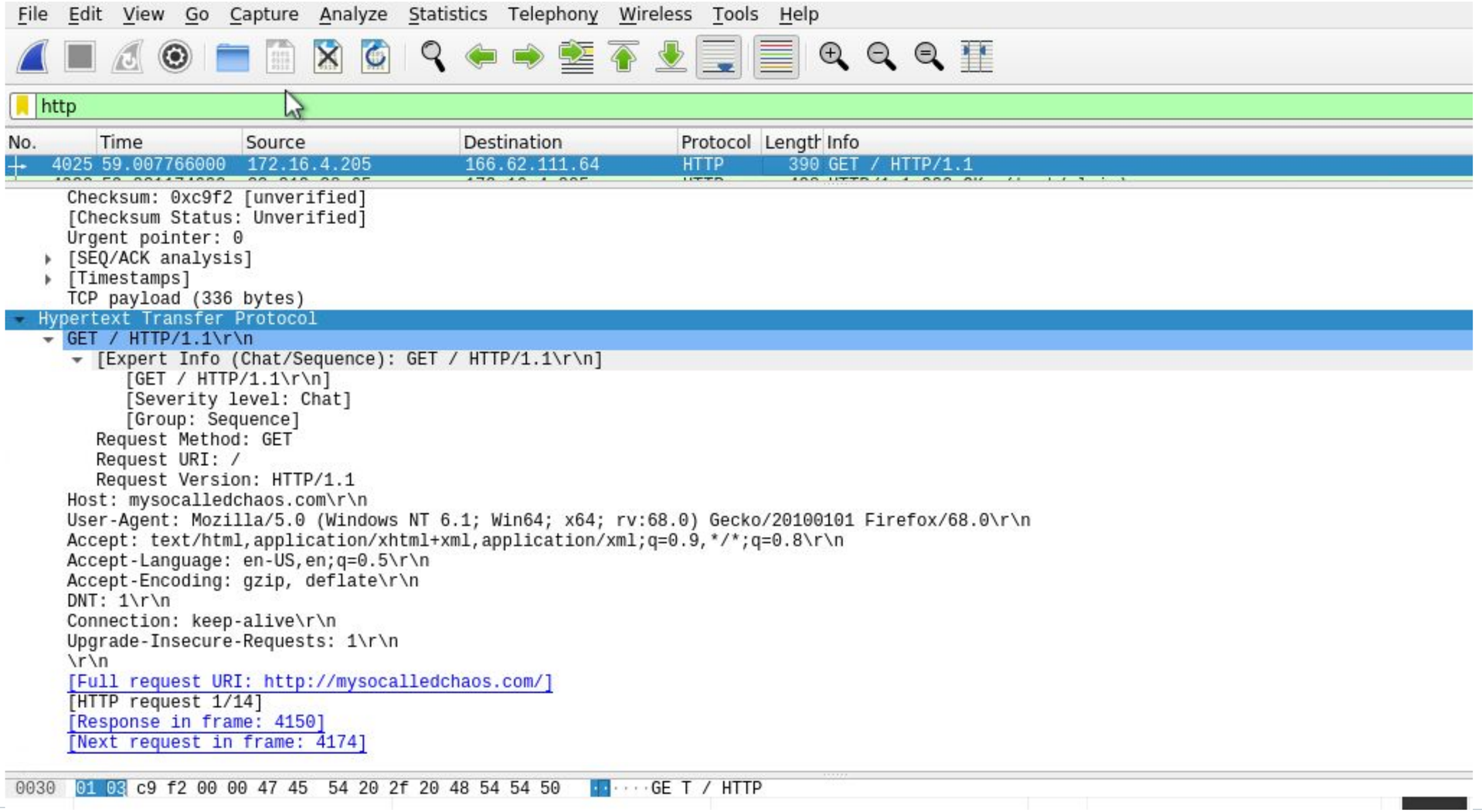


Normal Activity

Browsing the internet.

This behaviour used the ‘HTTP GET’ protocol

- Browsing the website http://www.mysocalledchaos.com



Viewing an image from a webpage.

HTTP GET protocol response 200 OK

Viewing the image Travel.jpg from the website www.mysocalledchaos.com

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
10754	155.042551200	166.62.111.64	172.16.4.205	HTTP	1336	HTTP/1.1 200 OK (PNG)

```
    Response Phrase: OK
  Last-Modified: Mon, 01 Apr 2019 19:33:32 GMT\r\n
  ETag: "60479-5857d188a6007"\r\n
  Cache-Control: max-age=5184000\r\n
  Expires: Sat, 14 Sep 2019 11:35:11 GMT\r\n
  X-XSS-Protection: 1; mode=block\r\n
  X-Content-Type-Options: nosniff\r\n
  Content-Type: image/png\r\n
  X-Port: port_10069\r\n
  X-Cacheable: YES\r\n
  Content-Length: 394361\r\n
  Date: Fri, 19 Jul 2019 18:53:10 GMT\r\n
  Age: 285473\r\n
  X-Cache: cached\r\n
  X-Cache-Hit: HIT\r\n
  X-Backend: all_requests\r\n
  Accept-Ranges: bytes\r\n
  \r\n
  [HTTP response 8/9]
  [Time since request: 63.038939300 seconds]
  [Prev request in frame: 5597]
  [Prev response in frame: 6667]
  [Request in frame: 6689]
  [Next request in frame: 10760]
  [Next response in frame: 13145]
  [Request URI: http://mysocalledchaos.com/wp-content/uploads/2018/02/Travel.jpg]
  File Data: 394361 bytes
```

Malicious Activity

Suspicious HTTP GET Request

SRC: LAPTOP-5WKHX9YG.frank-n-ted.com
DST: 205.185.125.104
REQ: HTTP GET /files/june11.dll

Analysis:

This activity is considered suspicious as the user has requested a ‘system’ file (DLL) from an unknown host (205.185.125.104).

Further analysis reveals notable RST packets from the DC, prior to the GET request. This suggests a malicious entity may already be at work.

A copy of the suspected malicious file was submitted to Virustotal, which once again reported a Trojan.

658.578232500	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	274 49738	389	SASL GSS-API Integrity: searchRequest(11) "CN=62a0ff2e-97b9-4513-943f-0d221bd30080,CN=Device
658.583037600	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	LDAP	300 389	49738	SASL GSS-API Integrity: searchResDone(11) noSuchObject (0000208D: NameErr: DSID-03100288, pro
658.584591600	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	97 49738	389	SASL GSS-API Integrity: unbindRequest(12)
658.585452200	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	54 49738	389	49738 → 389 [FIN, ACK] Seq=2309 Ack=3557 Win=262400 Len=0
658.586312200	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	54 389	49738	389 → 49738 [RST, ACK] Seq=3557 Ack=2309 Win=0 Len=0
658.587178100	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	54 389	49738	389 → 49738 [RST] Seq=3557 Win=0 Len=0
658.588727200	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	97 49737	389	SASL GSS-API Integrity: unbindRequest(13)
658.589593300	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	54 389	49737	389 → 49737 [RST, ACK] Seq=3488 Ack=2801 Win=0 Len=0
658.590452700	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	54 49737	389	49737 → 389 [FIN, ACK] Seq=2801 Ack=3488 Win=261888 Len=0
658.591319200	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	54 389	49737	389 → 49737 [RST] Seq=3488 Win=0 Len=0
658.592186900	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	54 49735	135	49735 → 135 [RST, ACK] Seq=497 Ack=453 Win=0 Len=0
658.593047000	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	54 49736	49667	49736 → 49667 [RST, ACK] Seq=3609 Ack=1838 Win=0 Len=0
658.615056700	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	TCP	66 49739	80	49739 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
658.615975900	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	58 80	49739	80 → 49739 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
658.616839000	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	TCP	54 49739	80	49739 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
658.621258400	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	275 49739	80	GET /pQBtWj HTTP/1.1
658.622127100	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	54 80	49739	80 → 49739 [ACK] Seq=1 Ack=222 Win=64240 Len=0
658.630781400	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP	542 80	49739	HTTP/1.1 302 Found
658.631653800	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	TCP	54 49739	80	49739 → 80 [ACK] Seq=222 Ack=489 Win=65535 Len=0
658.636633700	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	312 49739	80	GET /files/june11.dll HTTP/1.1
658.637670700	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	54 80	49739	80 → 49739 [ACK] Seq=489 Ack=480 Win=64240 Len=0
658.661748100	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	TCP	1514 80	49739	80 → 49739 [ACK] Seq=489 Ack=480 Win=64240 Len=1460 [TCP segment of a reassembled PDU]

Suspicious Communication & POST Request

SRC: 172.16.4.205
DST: 185.243.115.84
REQ: HTTP POST /empty.gif?ss&ss2img

Analysis:

Logs show 172.16.4.205 communicating with 185.243.115.84 via a persistent connection, suggestive that an application is maintaining the connection.

Several POST requests are once again seen, 2 including a screenshot of the 172.16.4.205 desktop.

ip.addr==185.243.115.84 && http.request.method == POST

Packet list | Narrow & Wide | Case sensitive | Display filter | ip.addr==185.243.115.84

Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
196.168142500	Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutions.co	HTTP	126	49249	80	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
196.795147600	Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutions.co	HTTP	534	49249	80	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
335.615005700	Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutions.co	HTTP	326	49249	80	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
398.455630400	Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutions.co	HTTP	496	49249	80	POST /empty.gif?ss&ss1img HTTP/1.1 (PNG)
461.182108400	Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutions.co	HTTP	1366	49249	80	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)

FIN