Wireshark HackTheBox Intro to Network Traffic Analysis

Avataris12 · Follow

2 min read · Aug 8, 2022

Listen Share More

Analysis with Wireshark

True or False: Wireshark can run on both Windows and Linux.

True

Which Pane allows a user to see a summary of each packet grabbed during the capture?

Packet List

Which pane provides you insight into the traffic you captured and displays it in both ASCII and Hex?

Packet Bytes

What switch is used with TShark to list possible interfaces to capture on?

-D

What switch allows us to apply filters in TShark?

-f

Is a capture filter applied before the capture starts or after? (answer before or after)

before

Wireshark Advanced Usage

Which plugin tab can provide us with a way to view conversation metadata and even protocol breakdowns for the entire PCAP file?

Statistics

What plugin tab will allow me to accomplish tasks such as applying filters, following streams, and viewing expert info?

Analyze

What stream oriented Transport protocol enables us to follow and rebuild conversations and the included data?

tcp

True or False: Wireshark can extract files from HTTP traffic.

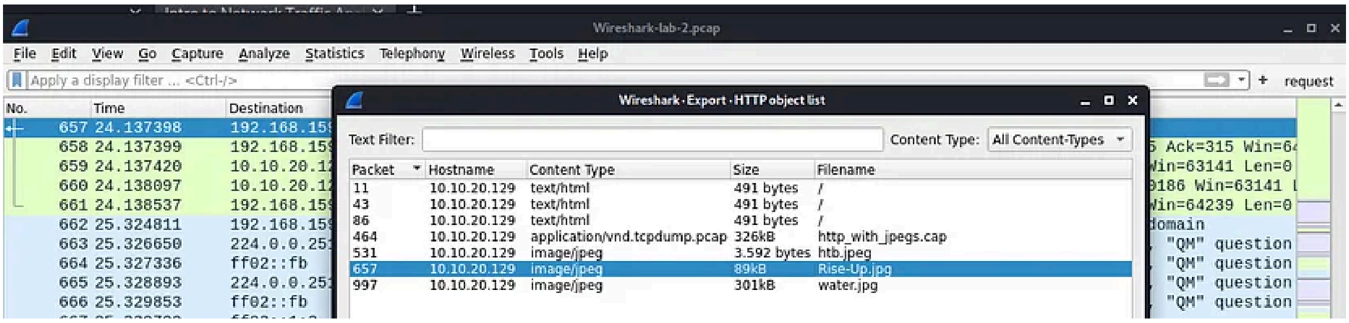
True

True or False: The ftp-data filter will show us any data sent over TCP port 21.

False

Packet Inception, Dissecting Network Traffic With Wireshark

> *unzip Wireshark-lab-2.zip*

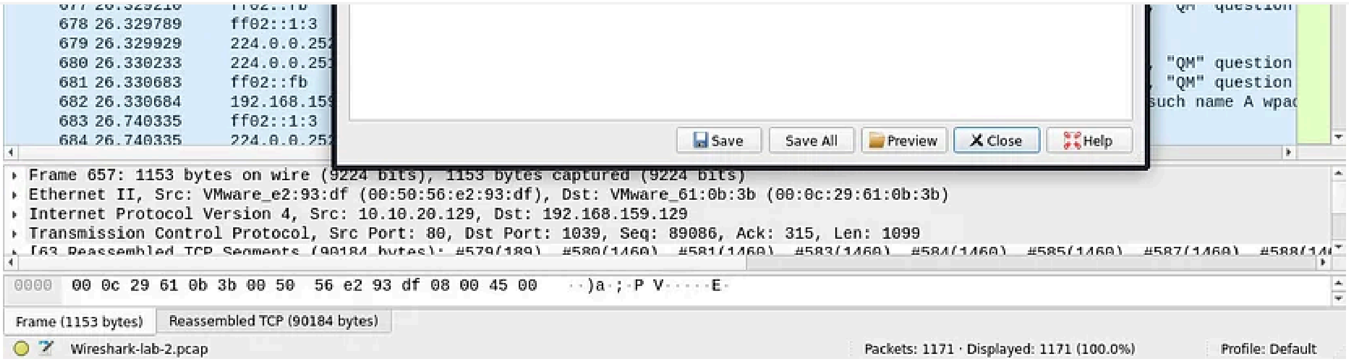

Wireshark-lab-2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
request
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
11	10.10.20.129	text/html	491 bytes	/
43	10.10.20.129	text/html	491 bytes	/
86	10.10.20.129	text/html	491 bytes	/
464	10.10.20.129	application/vnd.tcpdump.pcap	326kB	http_with_jpegs.cap
531	10.10.20.129	image/jpeg	3.592 bytes	htb.jpeg
657	10.10.20.129	image/jpeg	89kB	Rise-Up.jpg
997	10.10.20.129	image/jpeg	301kB	water.jpg

```
No.  Time        Destination
657 24.137398   192.168.159     5 Ack=315 Win=64
658 24.137399   192.168.159     Win=63141 Len=0
659 24.137420   10.10.20.12     9186 Win=63141 L
660 24.138097   10.10.20.12     Win=64239 Len=0
661 24.138537   192.168.159     domain
662 25.324811   192.168.159     "QM" question
663 25.326650   224.0.0.251     "QM" question
664 25.327336   ff02::fb        "QM" question
665 25.328893   224.0.0.251     "QM" question
666 25.329853   ff02::fb
```

Open in app ↗

Search



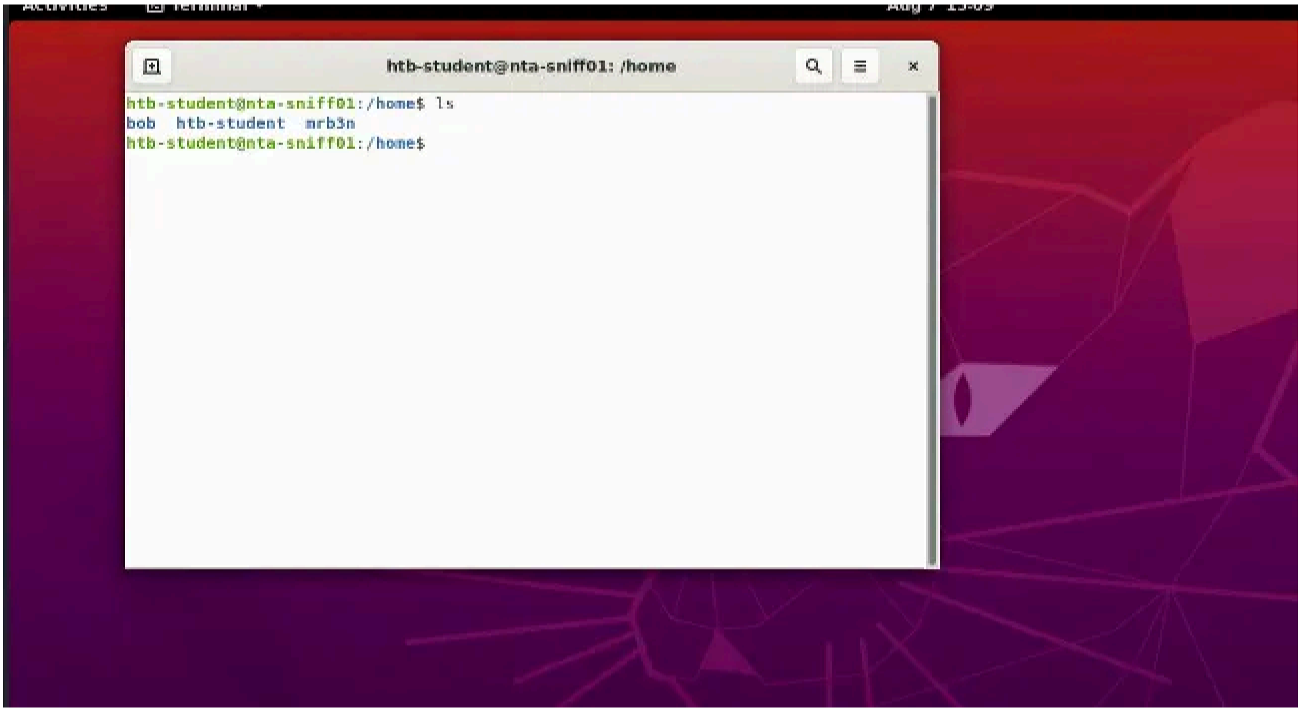
```
678 26.329789   ff02::1:3
679 26.329929   224.0.0.252      "QM" question
680 26.330233   224.0.0.251      "QM" question
681 26.330683   ff02::fb         such name A wpad
682 26.330684   192.168.159
683 26.740335   ff02::1:3
684 26.740335   224.0.0.252
```

```
› Frame 657: 1153 bytes on wire (9224 bits), 1153 bytes captured (9224 bits)
› Ethernet II, Src: VMware_e2:93:df (00:50:56:e2:93:df), Dst: VMware_61:0b:3b (00:0c:29:61:0b:3b)
› Internet Protocol Version 4, Src: 10.10.20.129, Dst: 192.168.159.129
› Transmission Control Protocol, Src Port: 80, Dst Port: 1039, Seq: 89086, Ack: 315, Len: 1099
› [63 Reassembled TCP Segments (90184 bytes): #579(189), #580(1460), #581(1460), #583(1460), #584(1460), #585(1460), #587(1460), #588(14

0000  00 0c 29 61 0b 3b 00 50  56 e2 93 df 08 00 45 00   ··)a·;·P V·····E·

Frame (1153 bytes)   Reassembled TCP (90184 bytes)
Wireshark-lab-2.pcap     Packets: 1171 · Displayed: 1171 (100.0%)     Profile: Default
```

What was the filename of the image that contained a certain Transformer Leader? (name.filetype)

Rise-Up.jpg

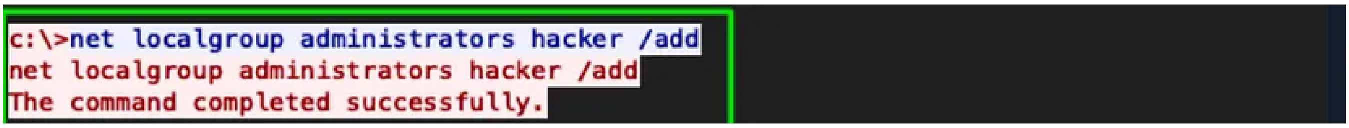
Which employee is suspected of performing potentially malicious actions in the live environment?



```
htb-student@nta-sniff01:/home$ ls
bob  htb-student  mrb3n
htb-student@nta-sniff01:/home$
```

Guided Lab: Traffic Analysis Workflow

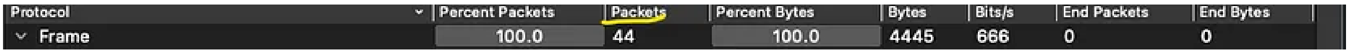
what was the name of the new user created on Mr. Ben's host?



```
c:\>net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.
```

hacker

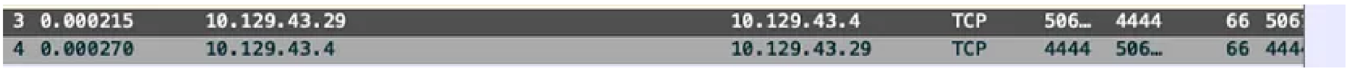
How many total packets were there in the Guided-analysis PCAP?



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Frame	100.0	44	100.0	4445	666	0	0

44

What was the suspicious port that was being used?



```
3 0.000215   10.129.43.29     10.129.43.4    TCP   506…  4444   66  506
4 0.000270   10.129.43.4      10.129.43.29   TCP   4444  506…   66  444
```

4444

Decrypting RDP connections

What user account was used to initiate the RDP connection?

bucky

Hackthebox Hackthebox Writeup Networking Network Security Ctf Writeup

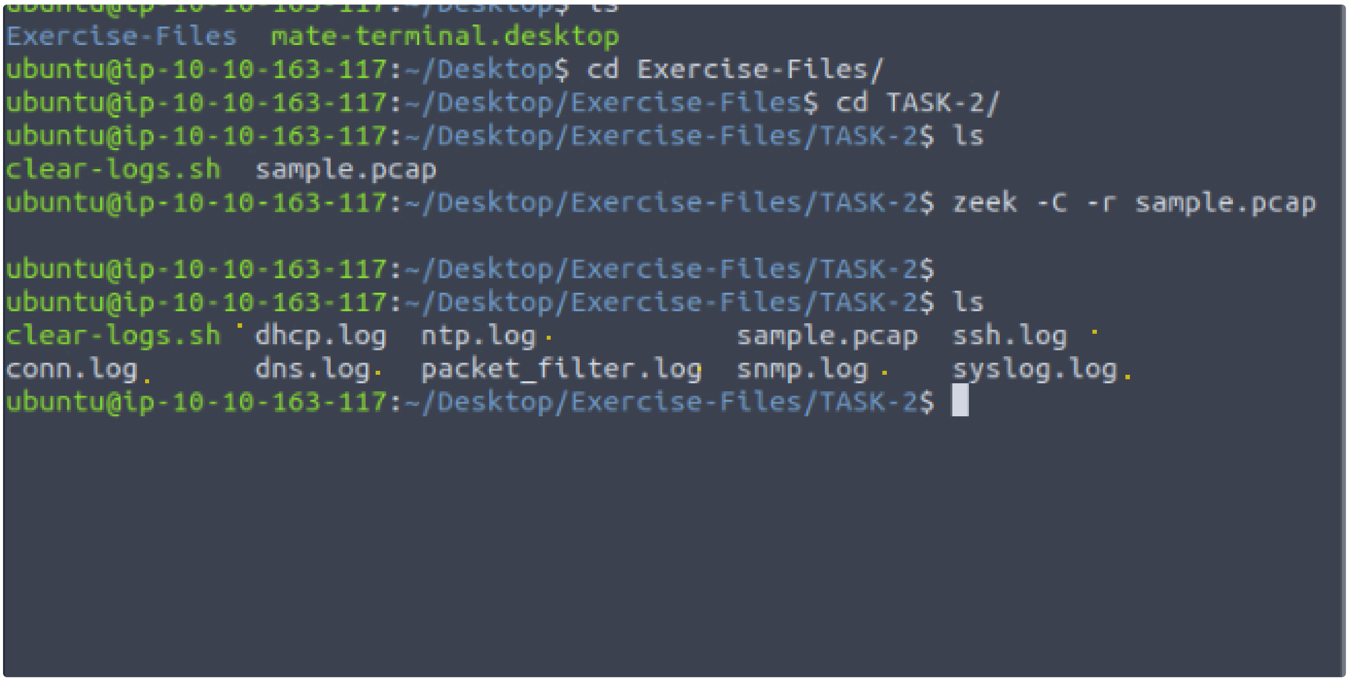
Follow

Written by Avataris12

570 Followers

Cybersecurity enthusiast, Airdrop Hunter

More from Avataris12



```
Exercise-Files  mate-terminal.desktop
ubuntu@ip-10-10-163-117:~/Desktop$ cd Exercise-Files/
ubuntu@ip-10-10-163-117:~/Desktop/Exercise-Files$ cd TASK-2/
ubuntu@ip-10-10-163-117:~/Desktop/Exercise-Files/TASK-2$ ls
clear-logs.sh  sample.pcap
ubuntu@ip-10-10-163-117:~/Desktop/Exercise-Files/TASK-2$ zeek -C -r sample.pcap

ubuntu@ip-10-10-163-117:~/Desktop/Exercise-Files/TASK-2$
ubuntu@ip-10-10-163-117:~/Desktop/Exercise-Files/TASK-2$ ls
clear-logs.sh  dhcp.log  ntp.log           sample.pcap  ssh.log
conn.log       dns.log   packet_filter.log  snmp.log    syslog.log
ubuntu@ip-10-10-163-117:~/Desktop/Exercise-Files/TASK-2$
```

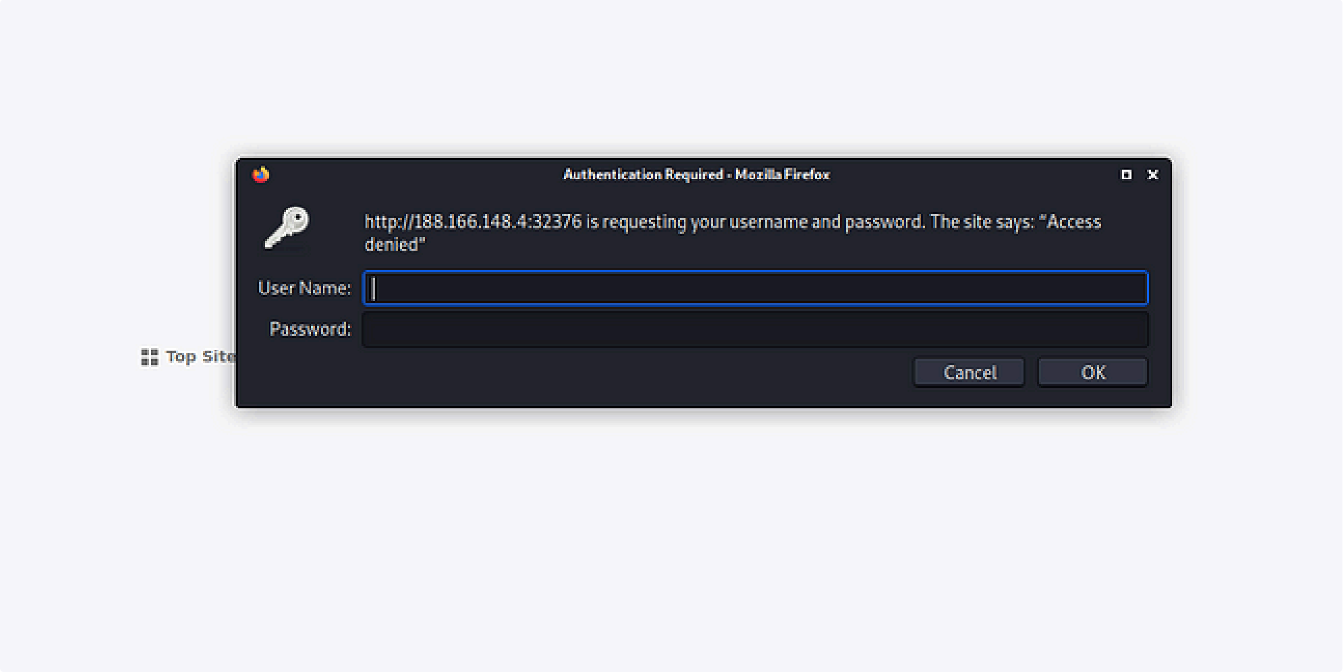
Avataris12

ZEEK TryHackMe writeup

Zeek is a free and open-source software network analysis framework.

5 min read · Aug 2, 2022

6



http://188.166.148.4:32376 is requesting your username and password. The site says: "Access denied"

User Name:

Password:

Avataris12

HTB Login Brute Forcing

Default Passwords

3 min read · Mar 21, 2022

9

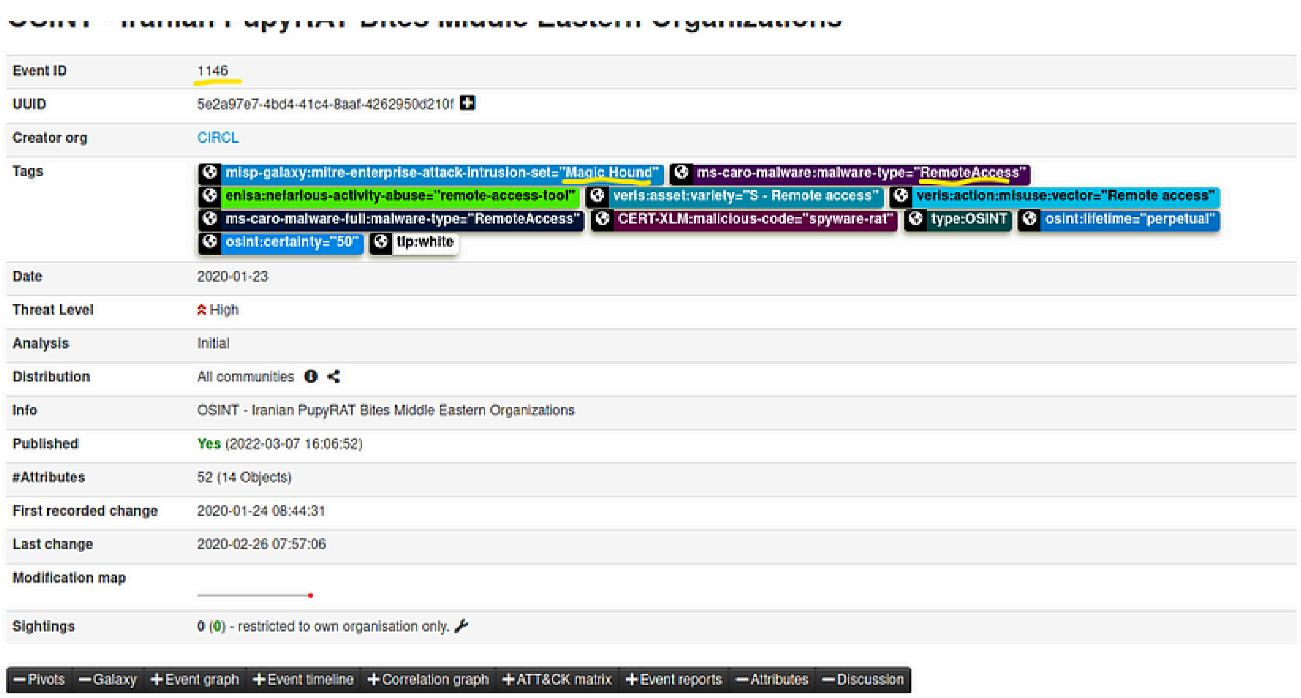
Avataris12

Intro to Network Traffic Analysis

Networking Primer — Layers 1–4

3 min read · Aug 8, 2022

2



OSINT - Iranian PupyRAT Bites Middle Eastern Organizations

Event ID	1146
UUID	5e2a97e7-4bd4-41c4-8aaf-4262950d210f
Creator org	CIRCL
Tags	misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound" ms-caro-malware:malware-type="RemoteAccess" enisa:nefarious-activity-abuse="remote-access-tool" veris:asset:variety="S - Remote access" veris:action:misuse:vector="Remote access" ms-caro-malware-full:malware-type="RemoteAccess" CERT-XLM:malicious-code="spyware-rat" type:OSINT osint:lifetime="perpetual" osint:certainty="50" tlp:white
Date	2020-01-23
Threat Level	High
Analysis	Initial
Distribution	All communities
Info	OSINT - Iranian PupyRAT Bites Middle Eastern Organizations
Published	Yes (2022-03-07 16:06:52)
#Attributes	52 (14 Objects)
First recorded change	2020-01-24 08:44:31
Last change	2020-02-26 07:57:06
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Avataris12

TryHackMe MISP

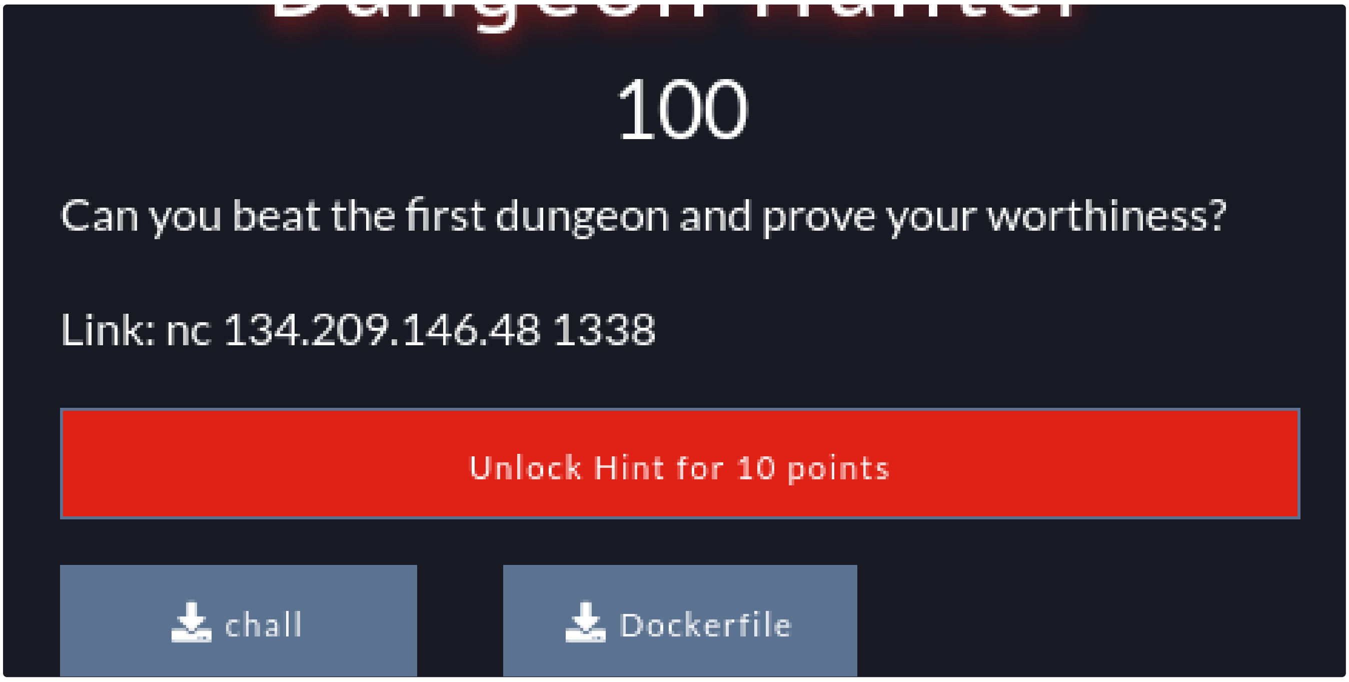
MISP—MALWARE INFORMATION SHARING PLATFORM

1 min read · Jul 31, 2022

53

See all from Avataris12

Recommended from Medium



Dungeon Hunter

100

Can you beat the first dungeon and prove your worthiness?

Link: nc 134.209.146.48 1338

Febin

Decode-E-Cyber CTF 2023—PWN/Binary Exploitation Writeup—1

I participated in Decode-E-Cyber CTF 2023 conducted by OWASP VIT Bhopal and we were the Winners! Team Pegasus with 1350 points. We were...

11 min read · Nov 7, 2023

142

Justin Mangaoang

Cyber Defenders: GitTheGate Blue Team Challenge Write-Up

Scenario:

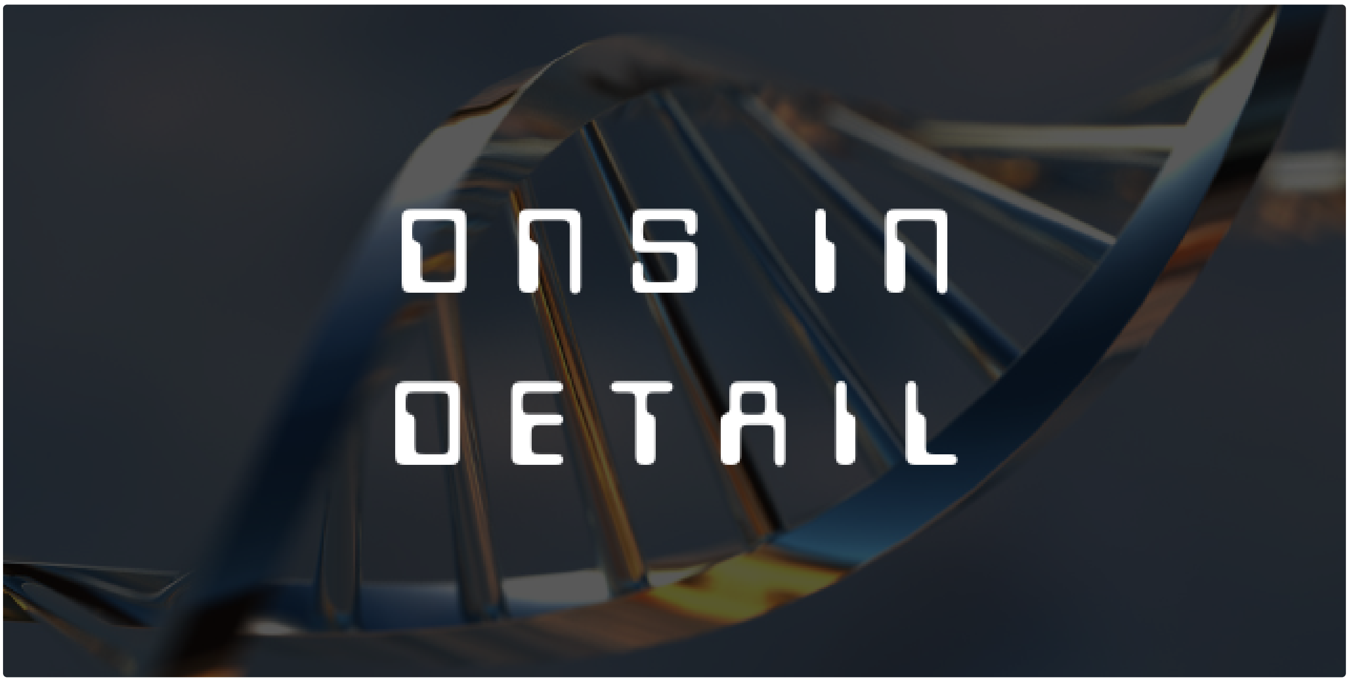
9 min read · Dec 23, 2023

21

Lists

Business 101

25 stories · 871 saves

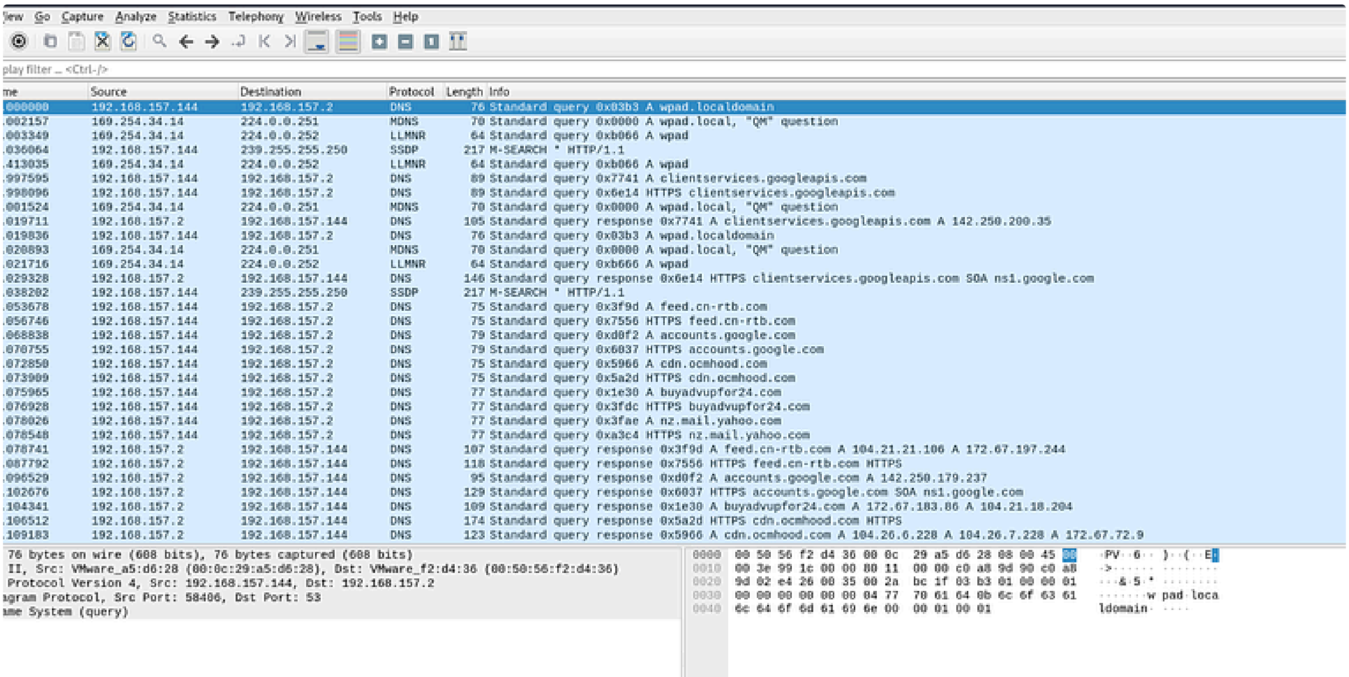


Hammaad M

TryHackMe, DNS In Detail

Learn how DNS works and how it helps you access internet services...

5 min read · Dec 7, 2023


iew Go Capture Analyze Statistics Telephony Wireless Tools Help
play filter … <Ctrl-/>

```
me          Source             Destination        Protocol  Length Info
.000000     192.168.157.144    192.168.157.2      DNS         76 Standard query 0x03b3 A wpad.localdomain
.002157     169.254.34.14      224.0.0.251        MDNS        70 Standard query 0x0000 A wpad.local, "QM" question
.003349     169.254.34.14      224.0.0.252        LLMNR       64 Standard query 0xb066 A wpad
.036064     192.168.157.144    239.255.255.250    SSDP       217 M-SEARCH * HTTP/1.1
.413035     169.254.34.14      224.0.0.252        LLMNR       64 Standard query 0xb066 A wpad
.997595     192.168.157.144    192.168.157.2      DNS         89 Standard query 0x7741 A clientservices.googleapis.com
.998096     192.168.157.144    192.168.157.2      DNS         89 Standard query 0x6e14 HTTPS clientservices.googleapis.com
.001524     169.254.34.14      224.0.0.251        MDNS        70 Standard query 0x0000 A wpad.local, "QM" question
.019711     192.168.157.2      192.168.157.144    DNS        105 Standard query response 0x7741 A clientservices.googleapis.com A 142.250.200.35
.019836     192.168.157.144    192.168.157.2      DNS         76 Standard query 0x03b3 A wpad.localdomain
.020893     169.254.34.14      224.0.0.251        MDNS        70 Standard query 0x0000 A wpad.local, "QM" question
.021716     169.254.34.14      224.0.0.252        LLMNR       64 Standard query 0xb666 A wpad
.029328     192.168.157.2      192.168.157.144    DNS        146 Standard query response 0x6e14 HTTPS clientservices.googleapis.com SOA ns1.google.com
.038202     192.168.157.144    239.255.255.250    SSDP       217 M-SEARCH * HTTP/1.1
.053678     192.168.157.144    192.168.157.2      DNS         75 Standard query 0x3f9d A feed.cn-rtb.com
.056746     192.168.157.144    192.168.157.2      DNS         75 Standard query 0x7556 HTTPS feed.cn-rtb.com
.068838     192.168.157.144    192.168.157.2      DNS         79 Standard query 0xd0f2 A accounts.google.com
.070755     192.168.157.144    192.168.157.2      DNS         79 Standard query 0x6037 HTTPS accounts.google.com
.072850     192.168.157.144    192.168.157.2      DNS         75 Standard query 0x5966 A cdn.ocmhood.com
.073909     192.168.157.144    192.168.157.2      DNS         75 Standard query 0x5a2d HTTPS cdn.ocmhood.com
.075965     192.168.157.144    192.168.157.2      DNS         77 Standard query 0x1e30 A buyadvupfor24.com
.076928     192.168.157.144    192.168.157.2      DNS         77 Standard query 0x3fdc HTTPS buyadvupfor24.com
.078026     192.168.157.144    192.168.157.2      DNS         77 Standard query 0x3fae A nz.mail.yahoo.com
.078548     192.168.157.144    192.168.157.2      DNS         77 Standard query 0xa3c4 HTTPS nz.mail.yahoo.com
.078741     192.168.157.2      192.168.157.144    DNS        107 Standard query response 0x3f9d A feed.cn-rtb.com A 104.21.21.106 A 172.67.197.244
.087792     192.168.157.2      192.168.157.144    DNS        118 Standard query response 0x7556 HTTPS feed.cn-rtb.com HTTPS
.096529     192.168.157.2      192.168.157.144    DNS         95 Standard query response 0xd0f2 A accounts.google.com A 142.250.179.237
.102676     192.168.157.2      192.168.157.144    DNS        129 Standard query response 0x6037 HTTPS accounts.google.com SOA ns1.google.com
.104341     192.168.157.2      192.168.157.144    DNS        109 Standard query response 0x1e30 A buyadvupfor24.com A 172.67.183.86 A 104.21.18.204
.106512     192.168.157.2      192.168.157.144    DNS        174 Standard query response 0x5a2d HTTPS cdn.ocmhood.com HTTPS
.109183     192.168.157.2      192.168.157.144    DNS        123 Standard query response 0x5966 A cdn.ocmhood.com A 104.26.6.228 A 104.26.7.228 A 172.67.72.9
```

```
 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
 II, Src: VMware_a5:d6:28 (00:0c:29:a5:d6:28), Dst: VMware_f2:d4:36 (00:50:56:f2:d4:36)
 Protocol Version 4, Src: 192.168.157.144, Dst: 192.168.157.2
agram Protocol, Src Port: 58406, Dst Port: 53
ame System (query)
```

```
0000  00 50 56 f2 d4 36 00 0c  29 a5 d6 28 08 00 45 00   ·PV··6·· )··(··E·
0010  00 3e 99 1c 00 00 80 11  00 00 c0 a8 9d 90 c0 a8   ·>······ ········
0020  9d 02 e4 26 00 35 00 2a  bc 1f 03 b3 01 00 00 01   ···&·5·* ········
0030  00 00 00 00 00 00 04 77  70 61 64 0b 6c 6f 63 61   ·······w pad·loca
0040  6c 64 6f 6d 61 69 6e 00  00 01 00 01               ldomain· ····
```

Genshi

Litter HackTheBox

Sherlock HackTheBox

4 min read · Dec 24, 2023

1

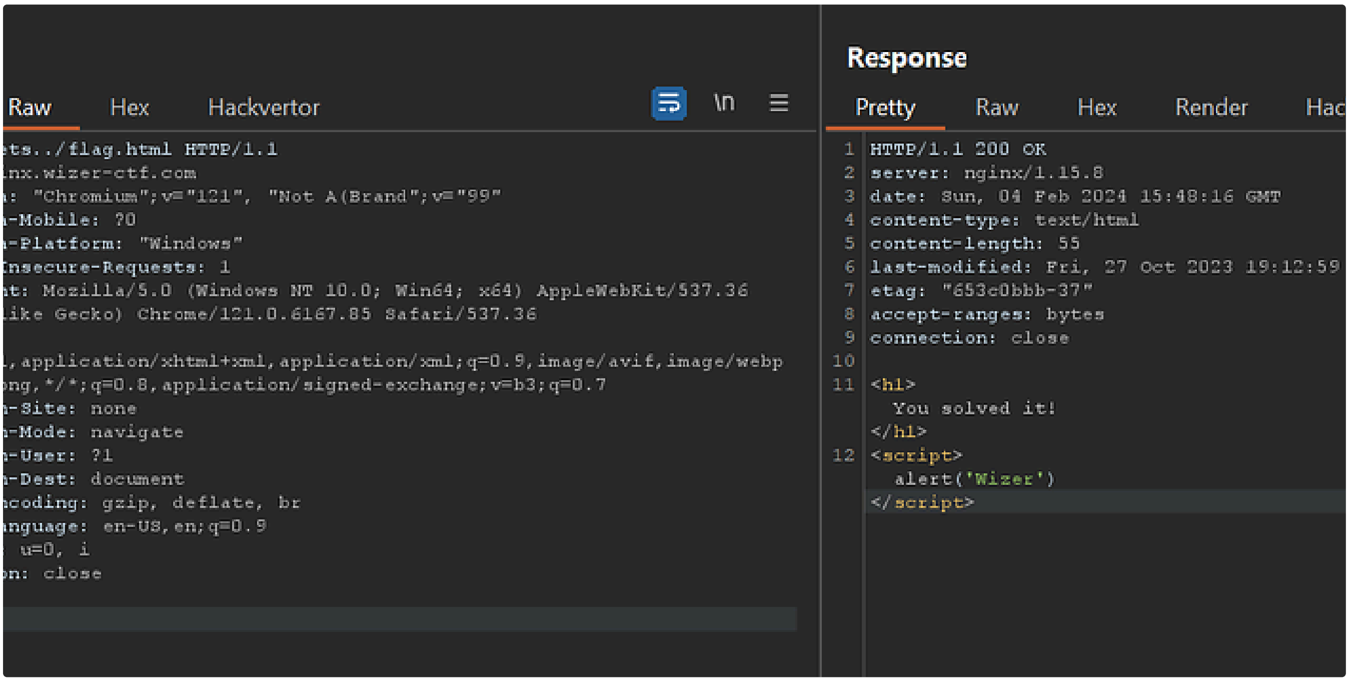
Salim Salimov

Hunting Malware in Sysmon Log with Splunk

Hello Medium,

11 min read · Nov 28, 2023

19 1



```
ets../flag.html HTTP/1.1
inx.wizer-ctf.com
a: "Chromium";v="121", "Not A(Brand";v="99"
a-Mobile: ?0
a-Platform: "Windows"
Insecure-Requests: 1
nt: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
like Gecko) Chrome/121.0.6167.85 Safari/537.36

l,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
a-Site: none
a-Mode: navigate
a-User: ?1
a-Dest: document
ncoding: gzip, deflate, br
nguage: en-US,en;q=0.9
: u=0, i
on: close
```

```
HTTP/1.1 200 OK
server: nginx/1.15.8
date: Sun, 04 Feb 2024 15:48:16 GMT
content-type: text/html
content-length: 55
last-modified: Fri, 27 Oct 2023 19:12:59
etag: "653c0bbb-37"
accept-ranges: bytes
connection: close

<h1>
  You solved it!
</h1>
<script>
  alert('Wizer')
</script>
```

Aftab Sama

Nginx Configuration - Wizer CTF

Through the Shelldon Cooper’s flag game website, with the following nginx configuration, get the flag from flag.html

2 min read · Feb 5, 2024

3

See more recommendations