BW3 es.7 Isolamento Host Compromesso tramite 5-Tuple

Esercizio Bonus 3: Isolamento Host Compromesso con 5-Tuple

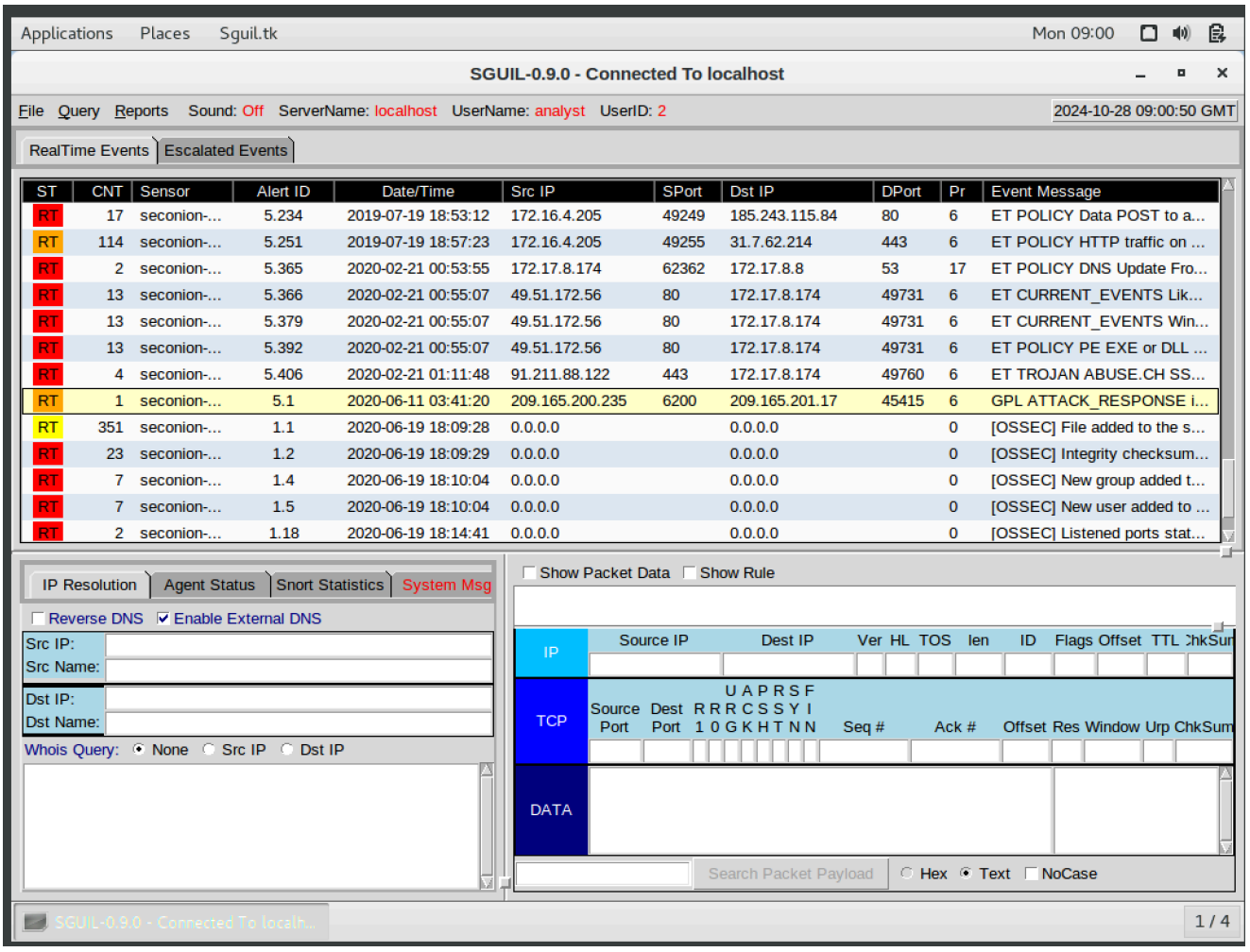
⚜️ **Tag:** #5tuple #isolamento_host #sguil #wireshark #kibana

---

Passaggio 1 - Esame degli Eventi su SGUIL

⚜️ **Tag:** #sguil #eventi #accesso_root

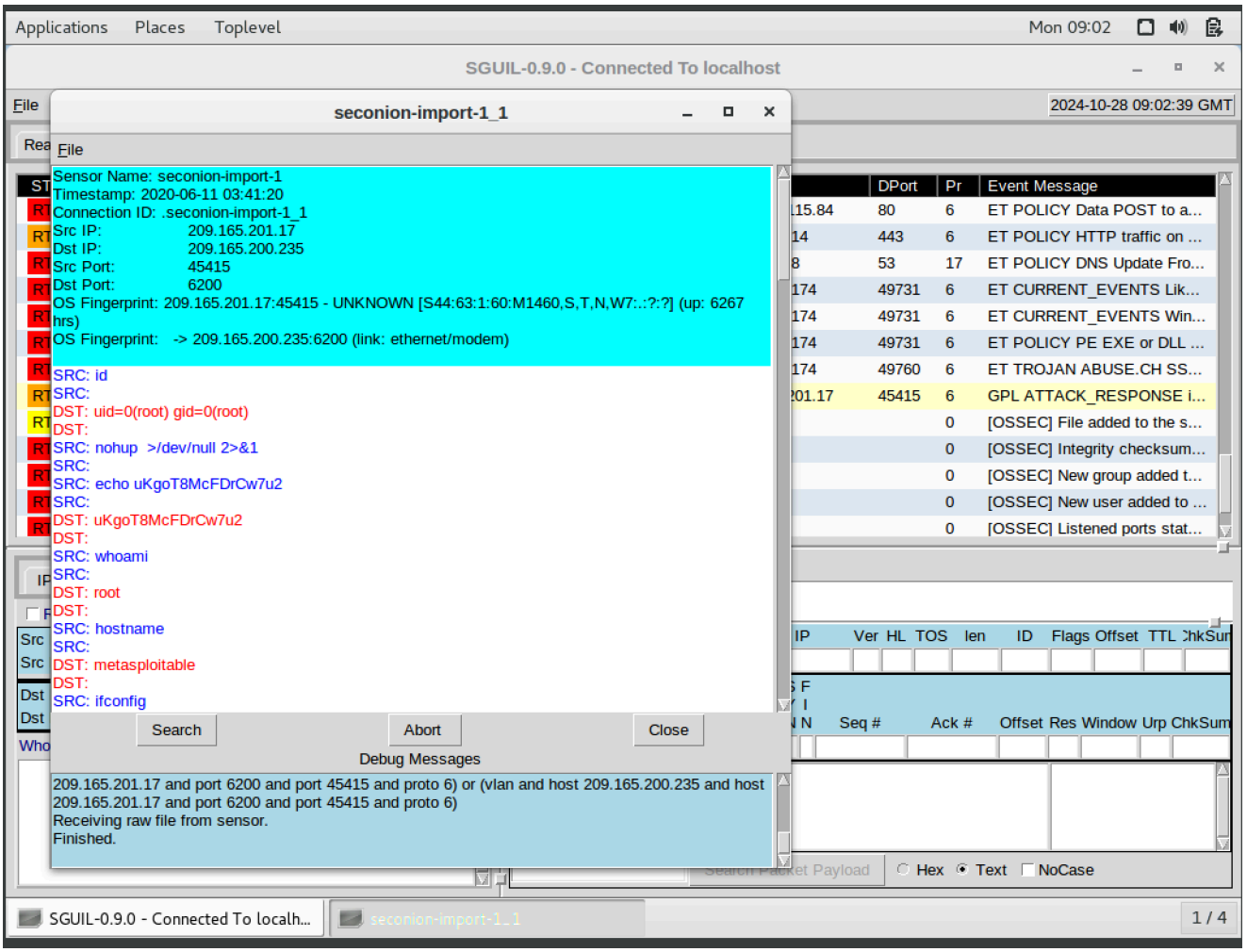
1. **Accesso a Security Onion**: Accedere alla macchina Security Onion con le credenziali (utente: analyst; password: cyberops).
2. **Avvio di SGUIL**: Analizzare gli eventi nella colonna **Messaggio Evento**, selezionando il messaggio **GPL ATTACK_RESPONSE id check turned root**, che indica un potenziale accesso root acquisito.
3. **Dettagli Pacchetto e Regola**: Selezionare **Mostra dati pacchetto** e **Mostra regola** per esaminare l’avviso in dettaglio.

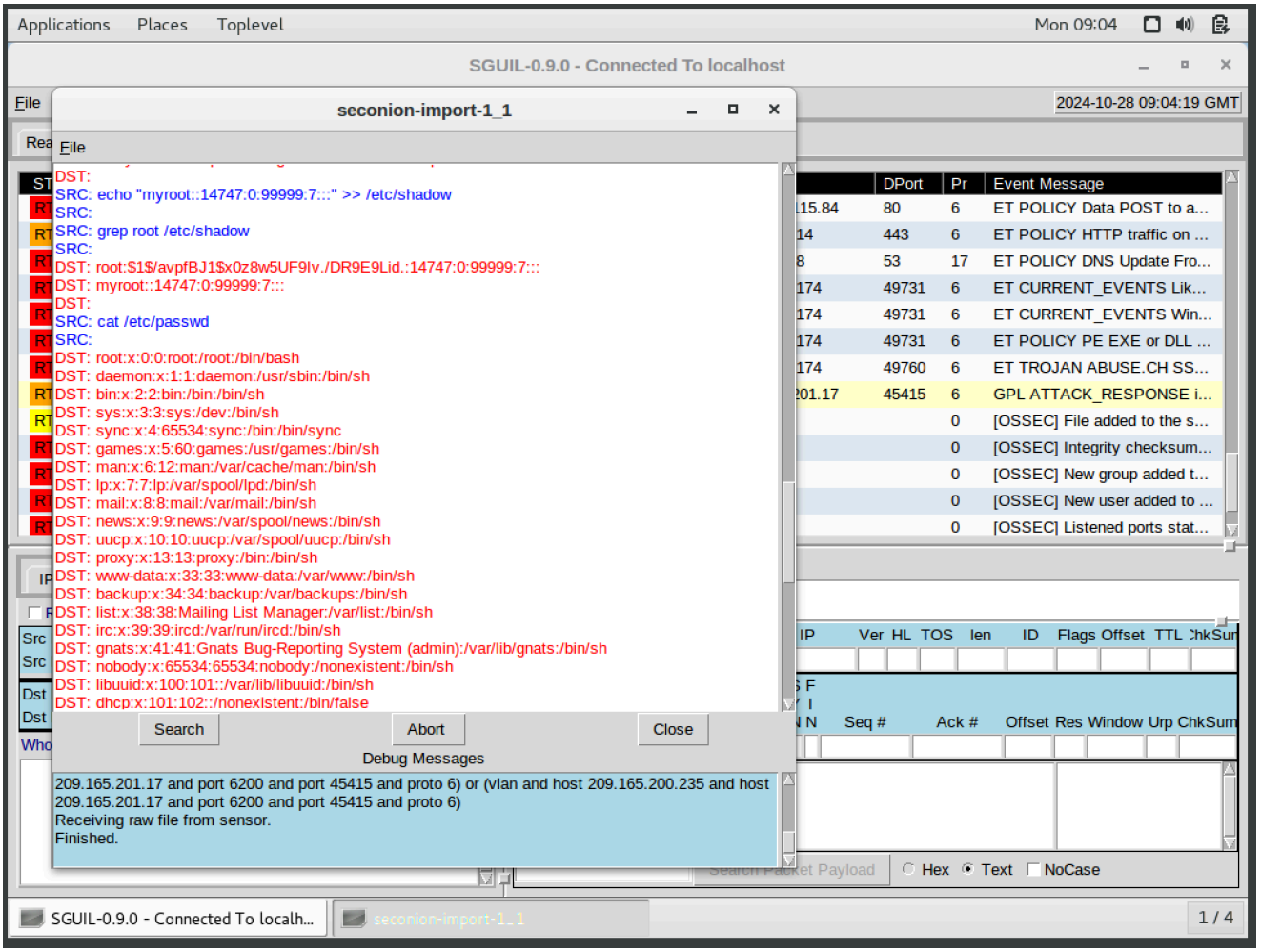


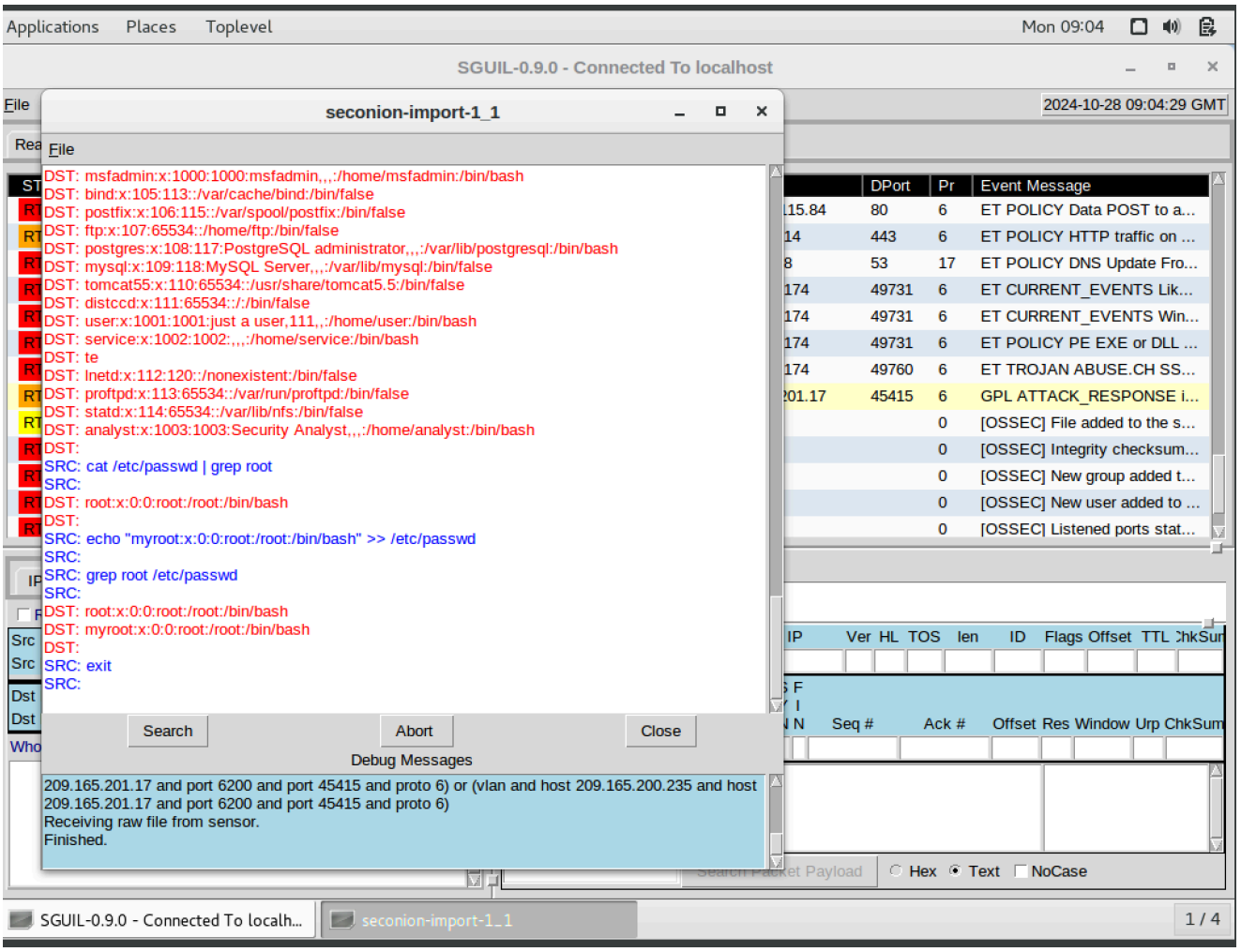
Passaggio 2 - Analisi delle Trascrizioni dell'Avviso

⚜️ **Tag:** #trascrizione #root_access #analisi_comandi

1. **Accesso alla Trascrizione**: Fare clic destro su **id 5.1** e selezionare **TRANSCRIPT**.
2. **Dettagli dell'Attacco**: Visualizzare la comunicazione tra attore minaccia (SRC) e target (DST), dove si osservano comandi Linux eseguiti sul target, accesso root acquisito, esplorazione del filesystem, copia e modifica di `/etc/shadow` e `/etc/passwd`.


Applications Places Toplevel
Mon 09:02
SGUIL-0.9.0 - Connected To localhost
File
2024-10-28 09:02:39 GMT
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
Search
Abort
Close
Debug Messages
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.
DPort Pr Event Message
80 6 ET POLICY Data POST to a...
443 6 ET POLICY HTTP traffic on ...
53 17 ET POLICY DNS Update Fro...
49731 6 ET CURRENT_EVENTS Lik...
49731 6 ET CURRENT_EVENTS Win...
49731 6 ET POLICY PE EXE or DLL ...
49760 6 ET TROJAN ABUSE.CH SS...
45415 6 GPL ATTACK_RESPONSE i...
0 [OSSEC] File added to the s...
0 [OSSEC] Integrity checksum...
0 [OSSEC] New group added t...
0 [OSSEC] New user added to ...
0 [OSSEC] Listened ports stat...
IP Ver HL TOS len ID Flags Offset TTL ChkSum
Seq # Ack # Offset Res Window Urp ChkSum
Hex Text NoCase
SGUIL-0.9.0 - Connected To localh...
seconion-import-1_1
1 / 4

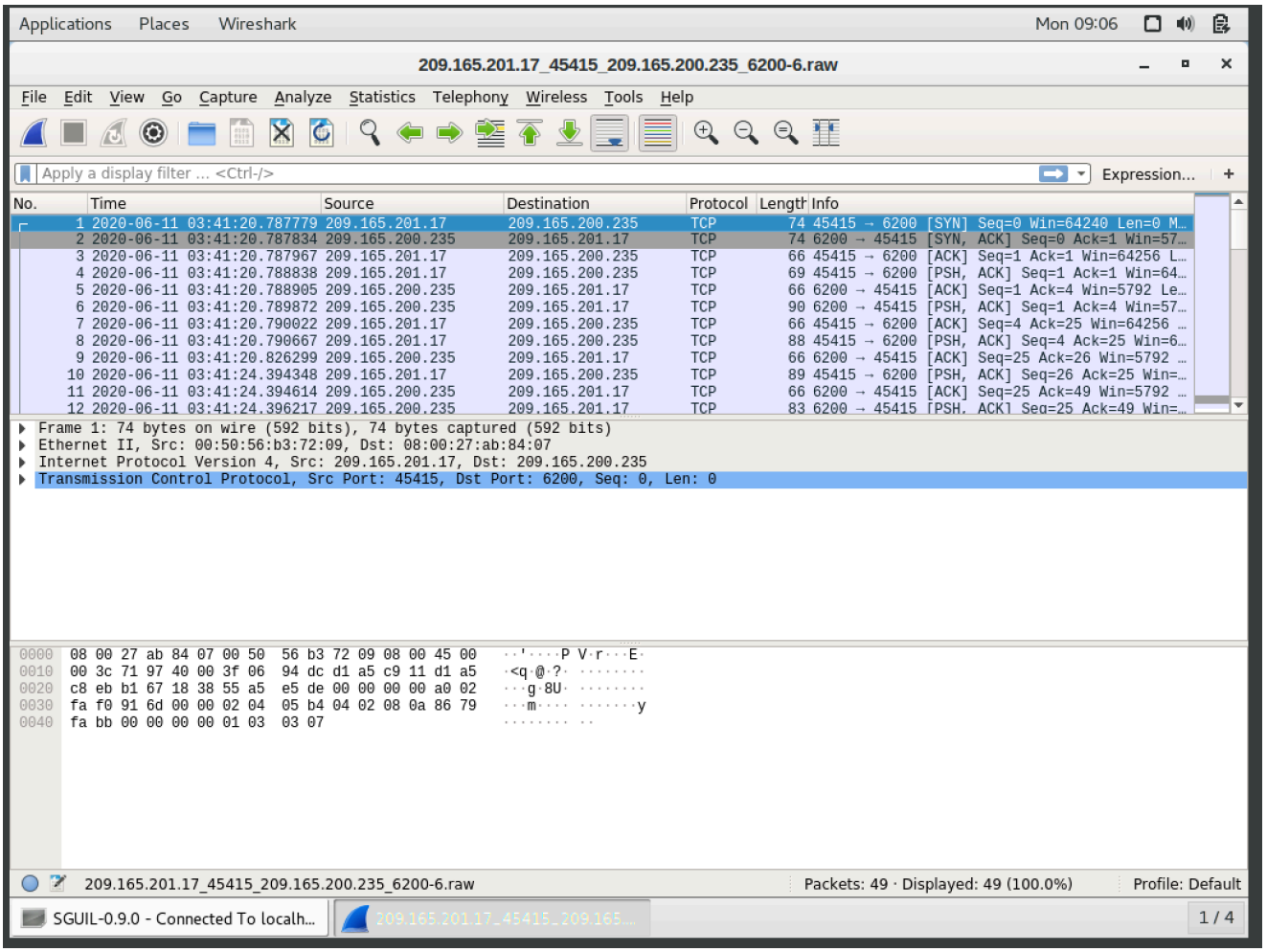

Applications Places Toplevel
Mon 09:04
SGUIL-0.9.0 - Connected To localhost
File
2024-10-28 09:04:19 GMT
seconion-import-1_1
File
DST:
SRC: echo "myroot::14747:0:99999:7:::" >> /etc/shadow
SRC:
SRC: grep root /etc/shadow
SRC:
DST: root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
DST: myroot::14747:0:99999:7:::
DST:
SRC: cat /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: daemon:x:1:1:daemon:/usr/sbin:/bin/sh
DST: bin:x:2:2:bin:/bin:/bin/sh
DST: sys:x:3:3:sys:/dev:/bin/sh
DST: sync:x:4:65534:sync:/bin:/bin/sync
DST: games:x:5:60:games:/usr/games:/bin/sh
DST: man:x:6:12:man:/var/cache/man:/bin/sh
DST: lp:x:7:7:lp:/var/spool/lpd:/bin/sh
DST: mail:x:8:8:mail:/var/mail:/bin/sh
DST: news:x:9:9:news:/var/spool/news:/bin/sh
DST: uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
DST: proxy:x:13:13:proxy:/bin:/bin/sh
DST: www-data:x:33:33:www-data:/var/www:/bin/sh
DST: backup:x:34:34:backup:/var/backups:/bin/sh
DST: list:x:38:38:Mailing List Manager:/var/list:/bin/sh
DST: irc:x:39:39:ircd:/var/run/ircd:/bin/sh
DST: gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
DST: nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
DST: libuuid:x:100:101::/var/lib/libuuid:/bin/sh
DST: dhcp:x:101:102::/nonexistent:/bin/false
Search
Abort
Close
Debug Messages
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.
DPort Pr Event Message
80 6 ET POLICY Data POST to a...
443 6 ET POLICY HTTP traffic on ...
53 17 ET POLICY DNS Update Fro...
49731 6 ET CURRENT_EVENTS Lik...
49731 6 ET CURRENT_EVENTS Win...
49731 6 ET POLICY PE EXE or DLL ...
49760 6 ET TROJAN ABUSE.CH SS...
45415 6 GPL ATTACK_RESPONSE i...
0 [OSSEC] File added to the s...
0 [OSSEC] Integrity checksum...
0 [OSSEC] New group added t...
0 [OSSEC] New user added to ...
0 [OSSEC] Listened ports stat...
IP Ver HL TOS len ID Flags Offset TTL ChkSum
Seq # Ack # Offset Res Window Urp ChkSum
Hex Text NoCase
SGUIL-0.9.0 - Connected To localh...
seconion-import-1_1
1 / 4

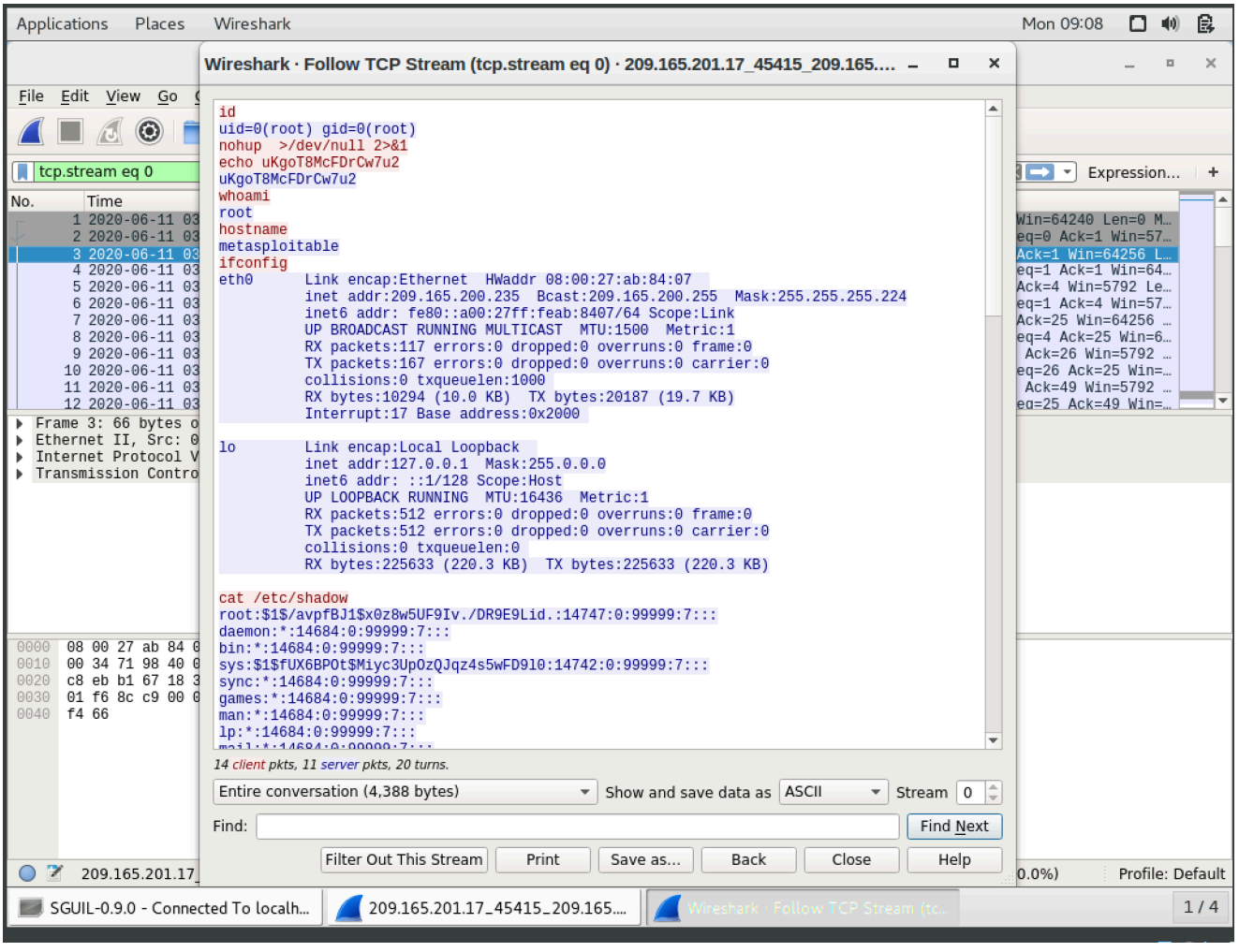


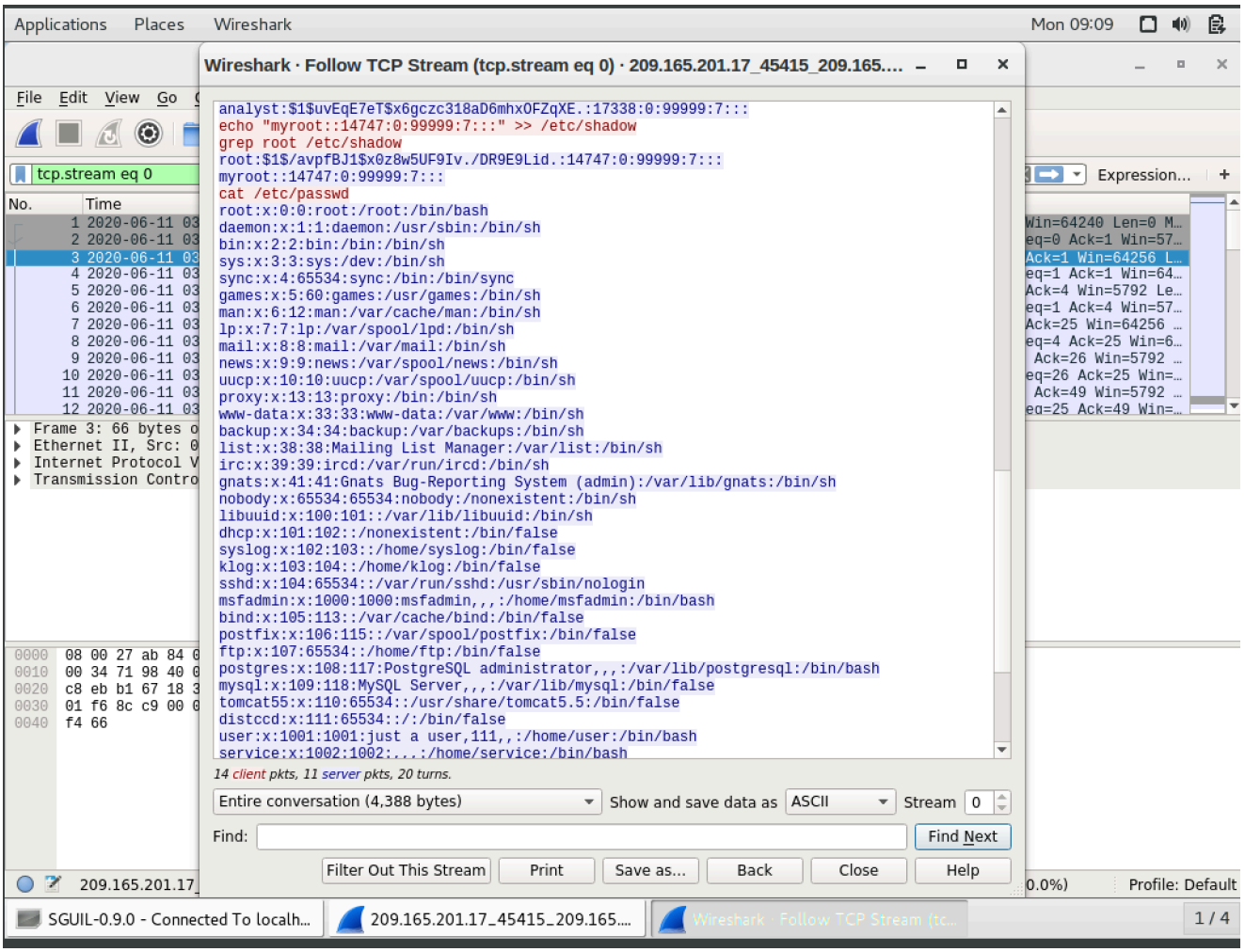
Passaggio 3 - Analisi in Wireshark

⚜️ **Tag:** #wireshark #tcp #flusso_dati

1. **Apertura in Wireshark**: Fare clic destro sull'ID dell'avviso e selezionare **Wireshark**.
2. **Analisi Flusso TCP**: Selezionare **Segui Flusso TCP** per esaminare la transazione tra attore minaccia (testo rosso) e target (testo blu). L'indirizzo IP del target è 209.165.200.235, con nome host "metasploitabile".


Applications Places Wireshark Mon 09:06
209.165.201.17_45415_209.165.200.235_6200-6.raw
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 2020-06-11 03:41:20.787779 209.165.201.17 209.165.200.235 TCP 74 45415 → 6200 [SYN] Seq=0 Win=64240 Len=0 M…
2 2020-06-11 03:41:20.787834 209.165.200.235 209.165.201.17 TCP 74 6200 → 45415 [SYN, ACK] Seq=0 Ack=1 Win=57…
3 2020-06-11 03:41:20.787967 209.165.201.17 209.165.200.235 TCP 66 45415 → 6200 [ACK] Seq=1 Ack=1 Win=64256 L…
4 2020-06-11 03:41:20.788838 209.165.201.17 209.165.200.235 TCP 69 45415 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=64…
5 2020-06-11 03:41:20.788905 209.165.200.235 209.165.201.17 TCP 66 6200 → 45415 [ACK] Seq=1 Ack=4 Win=5792 Le…
6 2020-06-11 03:41:20.789872 209.165.200.235 209.165.201.17 TCP 90 6200 → 45415 [PSH, ACK] Seq=1 Ack=4 Win=57…
7 2020-06-11 03:41:20.790022 209.165.201.17 209.165.200.235 TCP 66 45415 → 6200 [ACK] Seq=4 Ack=25 Win=64256 …
8 2020-06-11 03:41:20.790667 209.165.201.17 209.165.200.235 TCP 88 45415 → 6200 [PSH, ACK] Seq=4 Ack=25 Win=6…
9 2020-06-11 03:41:20.826299 209.165.200.235 209.165.201.17 TCP 66 6200 → 45415 [ACK] Seq=25 Ack=26 Win=5792 …
10 2020-06-11 03:41:24.394348 209.165.201.17 209.165.200.235 TCP 89 45415 → 6200 [PSH, ACK] Seq=26 Ack=25 Win=…
11 2020-06-11 03:41:24.394614 209.165.200.235 209.165.201.17 TCP 66 6200 → 45415 [ACK] Seq=25 Ack=49 Win=5792 …
12 2020-06-11 03:41:24.396217 209.165.200.235 209.165.201.17 TCP 83 6200 → 45415 [PSH, ACK] Seq=25 Ack=49 Win=…
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: 00:50:56:b3:72:09, Dst: 08:00:27:ab:84:07
Internet Protocol Version 4, Src: 209.165.201.17, Dst: 209.165.200.235
Transmission Control Protocol, Src Port: 45415, Dst Port: 6200, Seq: 0, Len: 0
0000 08 00 27 ab 84 07 00 50 56 b3 72 09 08 00 45 00
0010 00 3c 71 97 40 00 3f 06 94 dc d1 a5 c9 11 d1 a5
0020 c8 eb b1 67 18 38 55 a5 e5 de 00 00 00 00 a0 02
0030 fa f0 91 6d 00 00 02 04 05 b4 04 02 08 0a 86 79
0040 fa bb 00 00 00 00 01 03 03 07
209.165.201.17_45415_209.165.200.235_6200-6.raw
Packets: 49 · Displayed: 49 (100.0%)
Profile: Default
SGUIL-0.9.0 - Connected To localh...
1 / 4

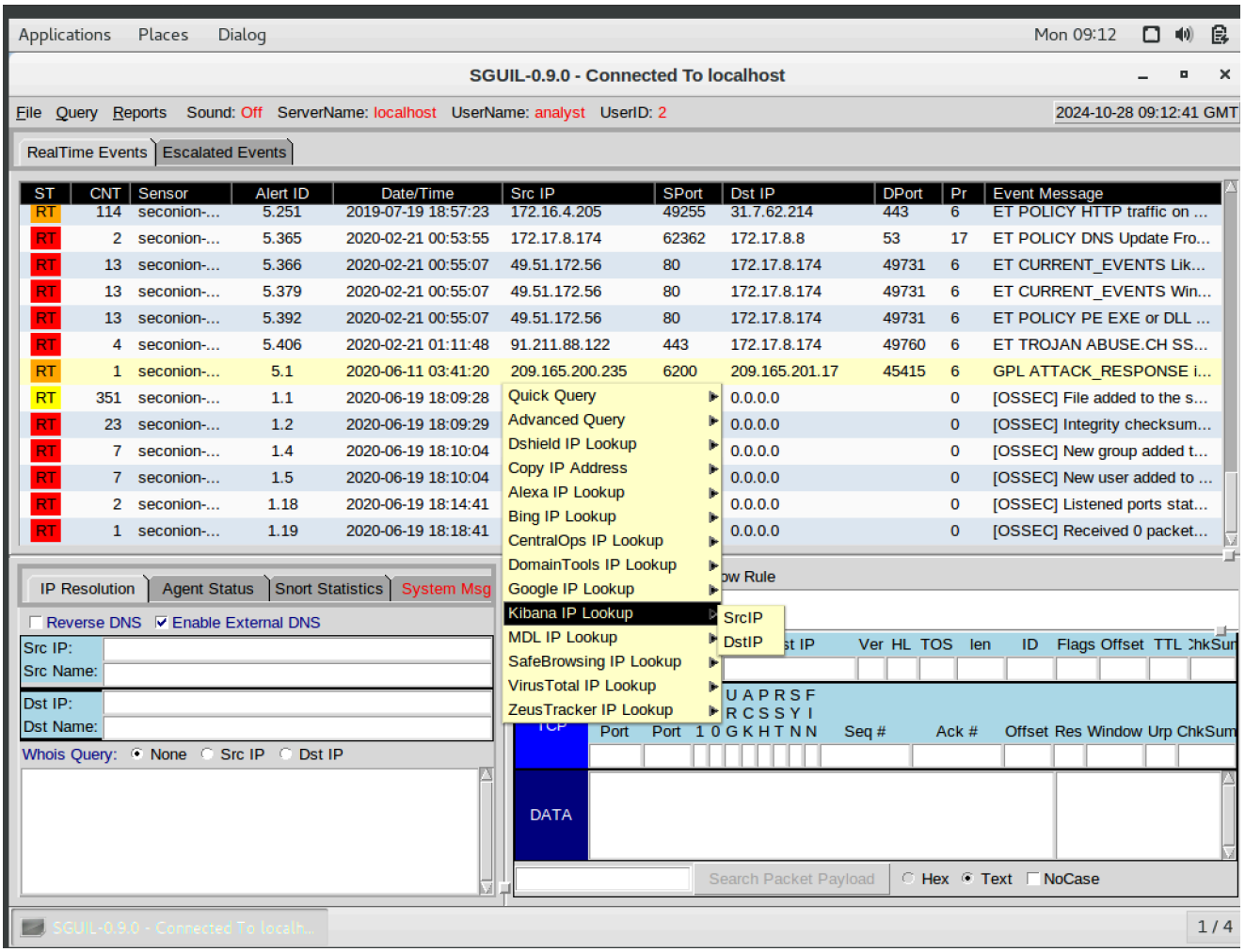

Applications Places Wireshark Mon 09:08
Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17_45415_209.165....
File Edit View Go
tcp.stream eq 0
Expression...
No. Time
id
uid=0(root) gid=0(root)
nohup >/dev/null 2>&1
echo uKgoT8McFDrCw7u2
uKgoT8McFDrCw7u2
whoami
root
hostname
metasploitable
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:ab:84:07
inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.255.224
inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:117 errors:0 dropped:0 overruns:0 frame:0
TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10294 (10.0 KB) TX bytes:20187 (19.7 KB)
Interrupt:17 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:512 errors:0 dropped:0 overruns:0 frame:0
TX packets:512 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:225633 (220.3 KB) TX bytes:225633 (220.3 KB)
cat /etc/shadow
root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
14 client pkts, 11 server pkts, 20 turns.
Entire conversation (4,388 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Profile: Default
SGUIL-0.9.0 - Connected To localh...
209.165.201.17_45415_209.165....
1 / 4



Passaggio 4 - Consultazione su Kibana

⚜️ **Tag:** #kibana #ip_lookup #analisi_temporale

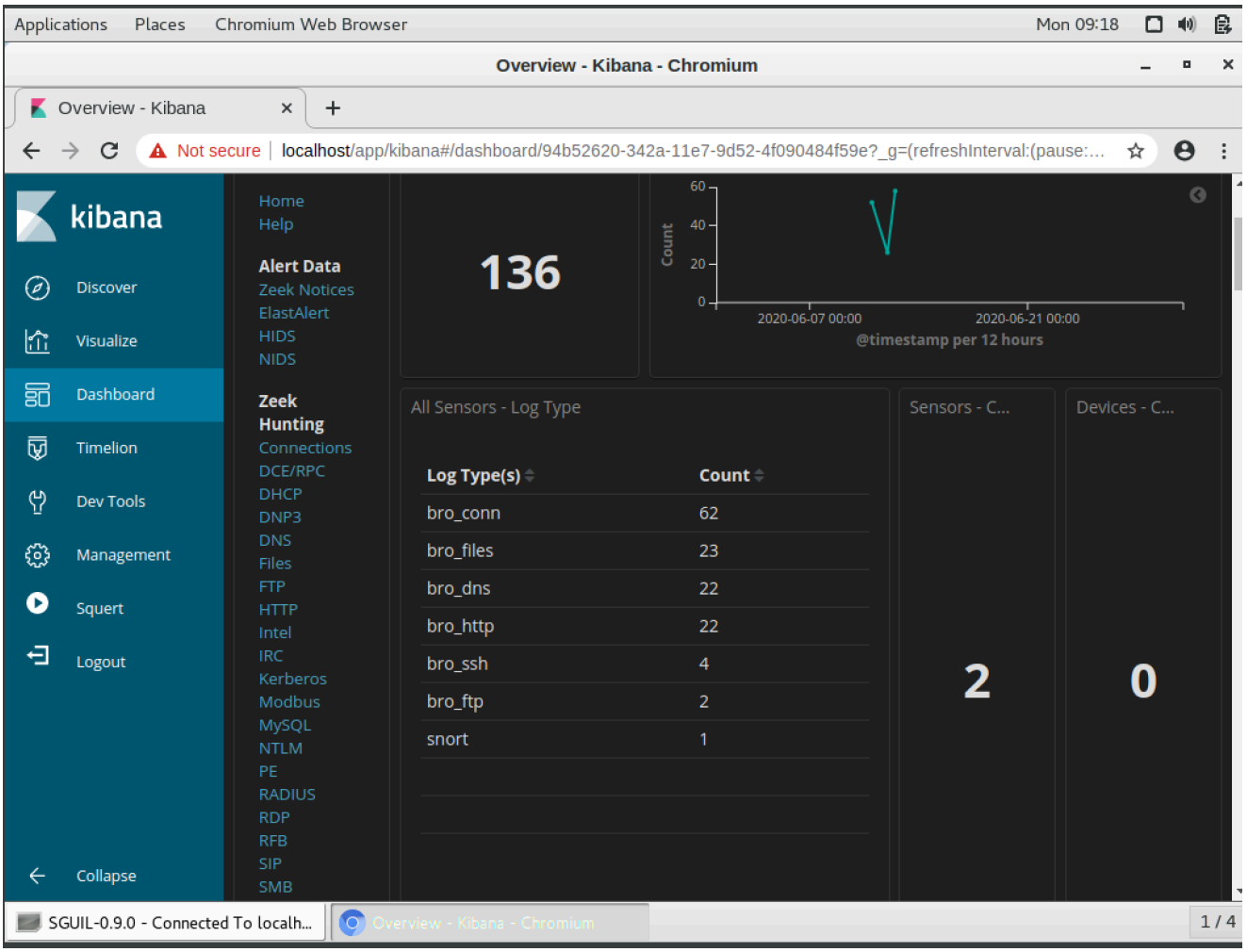
1. **Accesso al Lookup Kibana**: Tornare su SGUIL, fare clic destro sul **Source IP** e selezionare **KIBANA IP LOOKUP**.
2. **Impostazione Intervallo Temporale**: Modificare l'intervallo di tempo su **giugno 2020**.
3. **Analisi Protocolli di Trasferimento**: Filtrare per `bro_ftp` per confermare l'uso di FTP nel trasferimento del file **confidential.txt** rubato.

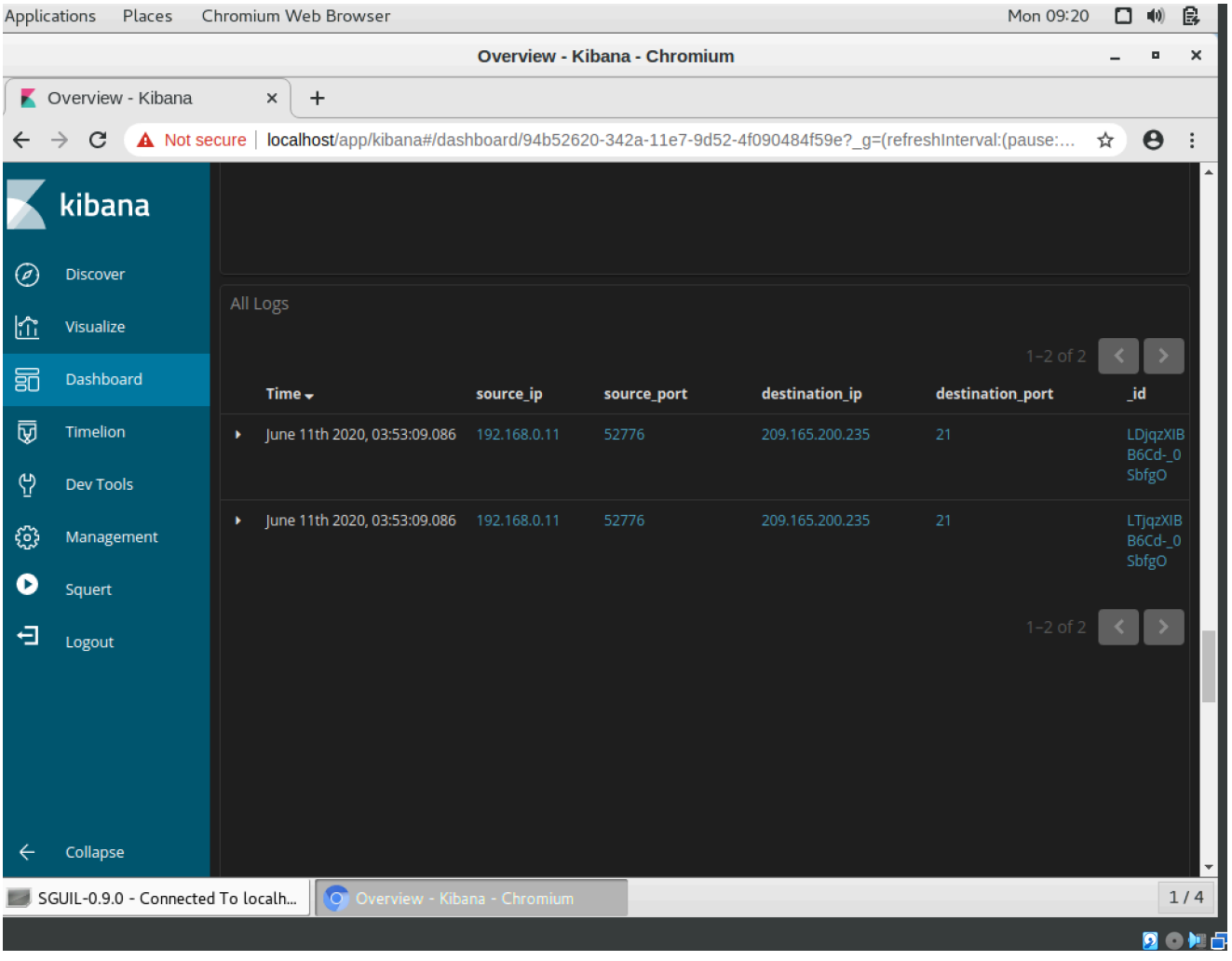


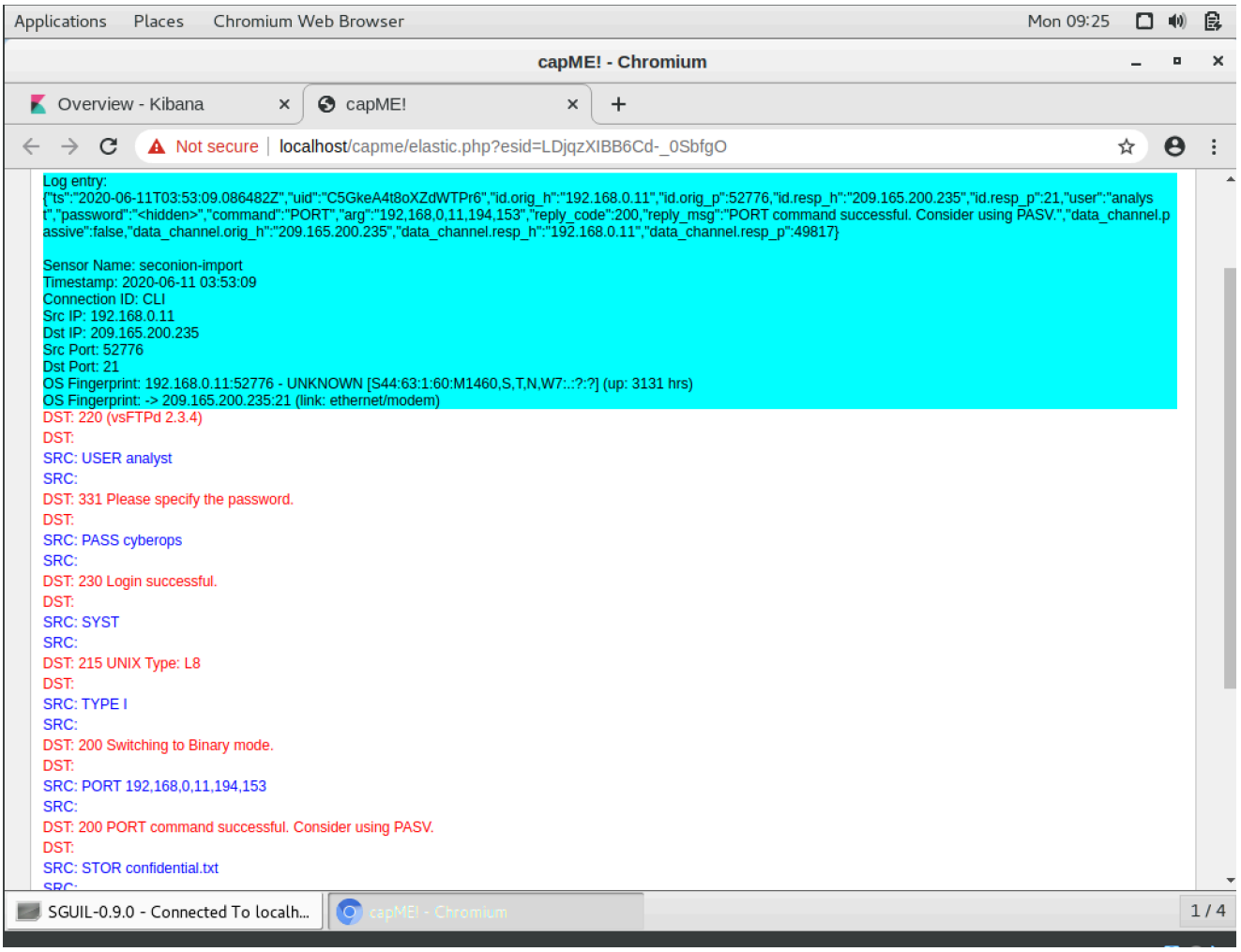
Passaggio 5 - Analisi dei File su Zeek

⚜️ **Tag:** #zeek #file_transfer #ftp

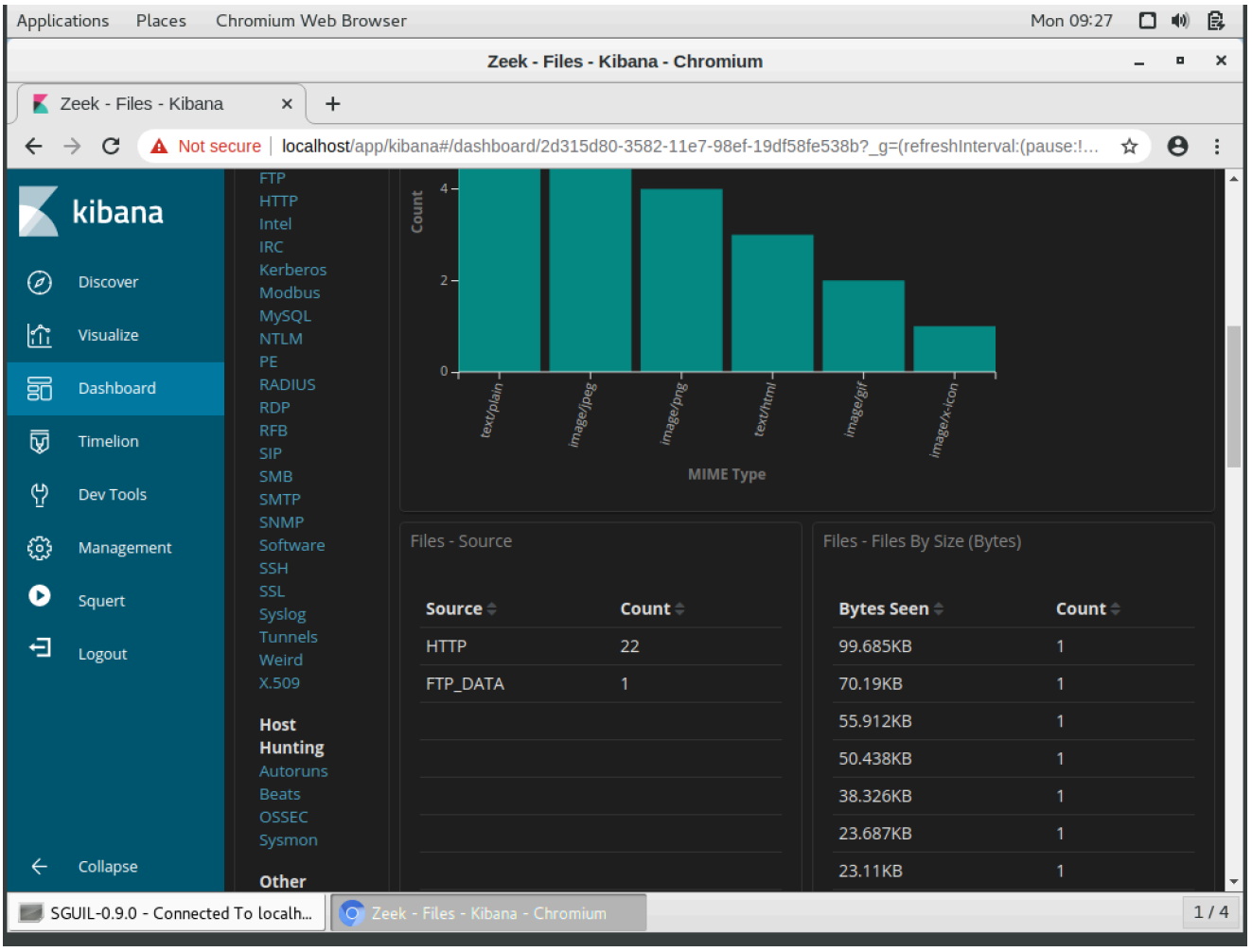
1. **Esame Tipi di File Registrati**: Dalla Dashboard di Kibana, selezionare **files** sotto **Zeek Hunting**.

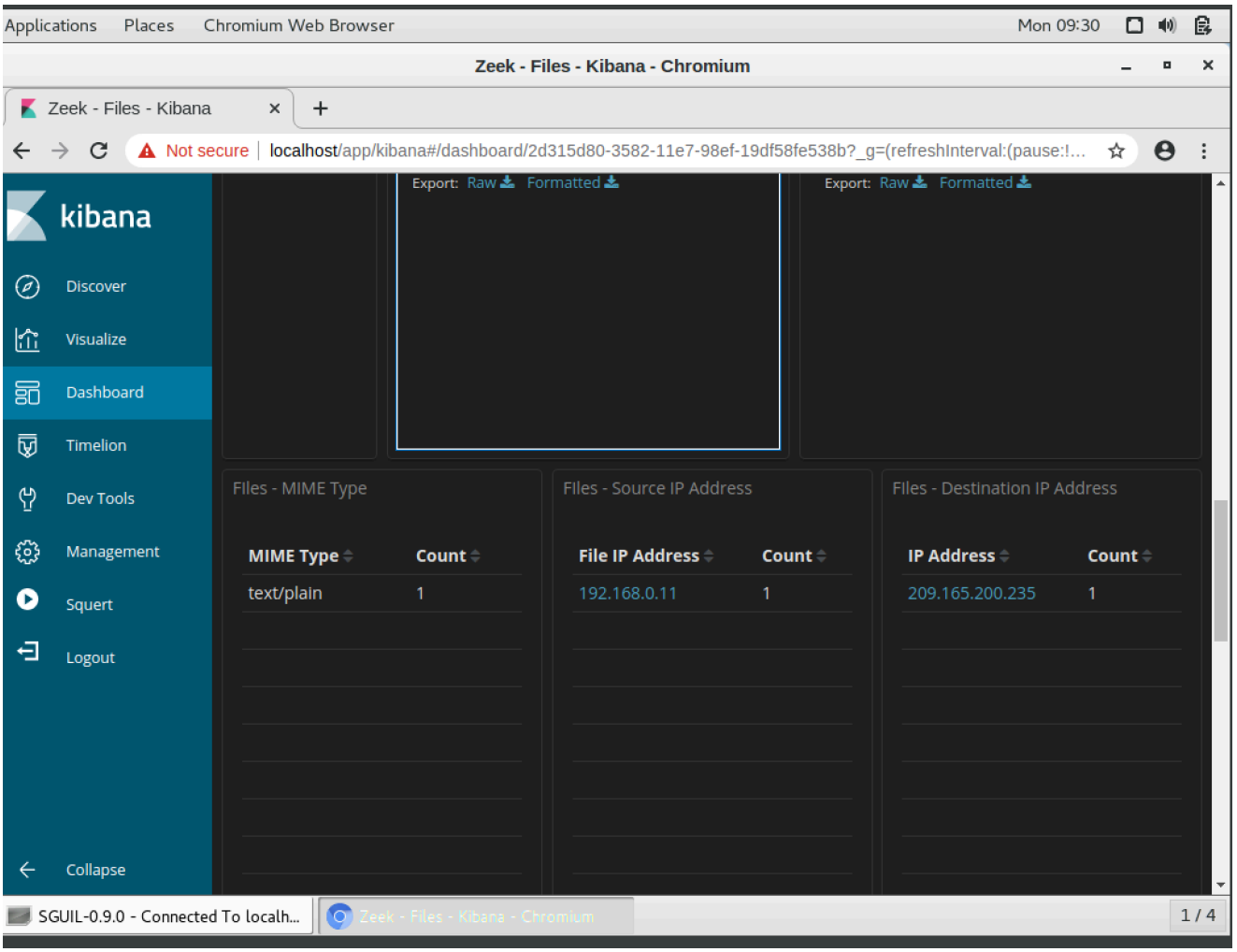

Applications Places Chromium Web Browser Mon 09:18
Overview - Kibana - Chromium
Overview - Kibana
Not secure | localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=(refreshInterval:(pause:...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
Home
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
136
Count
60
40
20
0
2020-06-07 00:00
2020-06-21 00:00
@timestamp per 12 hours
All Sensors - Log Type
Log Type(s)
Count
bro_conn 62
bro_files 23
bro_dns 22
bro_http 22
bro_ssh 4
bro_ftp 2
snort 1
Sensors - C...
2
Devices - C...
0
SGUIL-0.9.0 - Connected To localh...
Overview - Kibana - Chromium
1 / 4

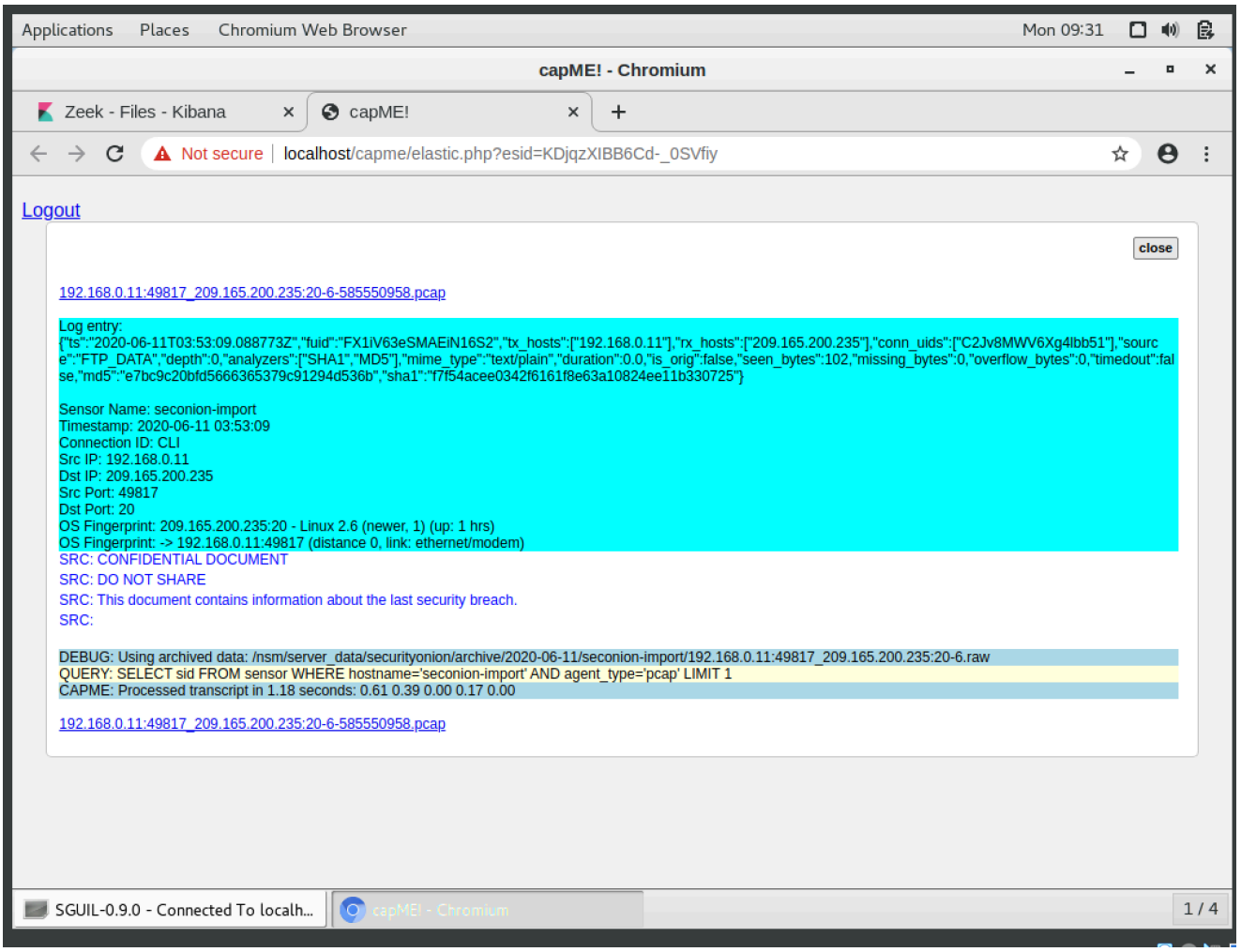

Applications Places Chromium Web Browser Mon 09:20
Overview - Kibana - Chromium
Overview - Kibana
Not secure | localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=(refreshInterval:(pause:...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
All Logs
1–2 of 2
Time
source_ip
source_port
destination_ip
destination_port
_id
June 11th 2020, 03:53:09.086 192.168.0.11 52776 209.165.200.235 21 LDjqzXIBB6Cd-_0SbfgO
June 11th 2020, 03:53:09.086 192.168.0.11 52776 209.165.200.235 21 LTjqzXIBB6Cd-_0SbfgO
1–2 of 2
SGUIL-0.9.0 - Connected To localh...
Overview - Kibana - Chromium
1 / 4



1. **Dettagli FTP**: Cliccare su FTP per identificare che il file trasferito è **confidential.txt**, inviato l'11 giugno 2020 alle 3:53 da 192.168.0.11 a 209.165.200.235.


Applications Places Chromium Web Browser Mon 09:27
Zeek - Files - Kibana - Chromium
Zeek - Files - Kibana
Not secure localhost/app/kibana#/dashboard/2d315d80-3582-11e7-98ef-19df58fe538b?_g=(refreshInterval:(pause:!...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
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
Count
4
2
0
text/plain
image/jpeg
image/png
text/html
image/gif
image/x-icon
MIME Type
Files - Source
Source
Count
HTTP
22
FTP_DATA
1
Files - Files By Size (Bytes)
Bytes Seen
Count
99.685KB
1
70.19KB
1
55.912KB
1
50.438KB
1
38.326KB
1
23.687KB
1
23.11KB
1
SGUIL-0.9.0 - Connected To localh...
Zeek - Files - Kibana - Chromium
1 / 4


Applications Places Chromium Web Browser Mon 09:30
Zeek - Files - Kibana - Chromium
Zeek - Files - Kibana
Not secure localhost/app/kibana#/dashboard/2d315d80-3582-11e7-98ef-19df58fe538b?_g=(refreshInterval:(pause:!...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
Export: Raw Formatted
Export: Raw Formatted
Files - MIME Type
MIME Type
Count
text/plain
1
Files - Source IP Address
File IP Address
Count
192.168.0.11
1
Files - Destination IP Address
IP Address
Count
209.165.200.235
1
SGUIL-0.9.0 - Connected To localh...
Zeek - Files - Kibana - Chromium
1 / 4



Raccomandazioni di Sicurezza

⚜️ **Tag:** #sicurezza #best_practices #2FA #password

1. **Autenticazione a Due Fattori (2FA)**: Implementare 2FA per gli account critici.
2. **Password Sicure**: Promuovere l'uso di password complesse e un sistema di gestione delle stesse.
3. **Limitazione dei Permessi**: Basare i permessi sul principio del minimo privilegio.
4. **Monitoraggio e Logging**: Attivare il logging degli accessi per individuare attività sospette.
5. **Aggiornamento e Patch**: Effettuare aggiornamenti regolari dei sistemi per ridurre le vulnerabilità.

6. **Formazione del Personale**: Sensibilizzare il personale sui rischi e le best practices di sicurezza.
7. **Crittografia dei Dati**: Applicare crittografia per proteggere i dati sensibili.

🔑 **Chiavi:**
[cybersecurity, isolamento_host, SGUIL, Wireshark, Kibana, autenticazione_due_fattori, password_sicure, logging, crittografia]

Suggerimenti per Approfondimenti

- **Automazione con Script per SGUIL**: Creare script Python per automatizzare il rilevamento di eventi specifici.
- **Integrazione di Zeek con Kibana**: Approfondire come Zeek può essere configurato per filtrare e analizzare specifici tipi di traffico.
- **Curiosità**: SGUIL e Kibana sono strumenti open-source potenti per il rilevamento e l’analisi di minacce in tempo reale, utilizzati da molte organizzazioni per migliorare la visibilità su reti complesse.