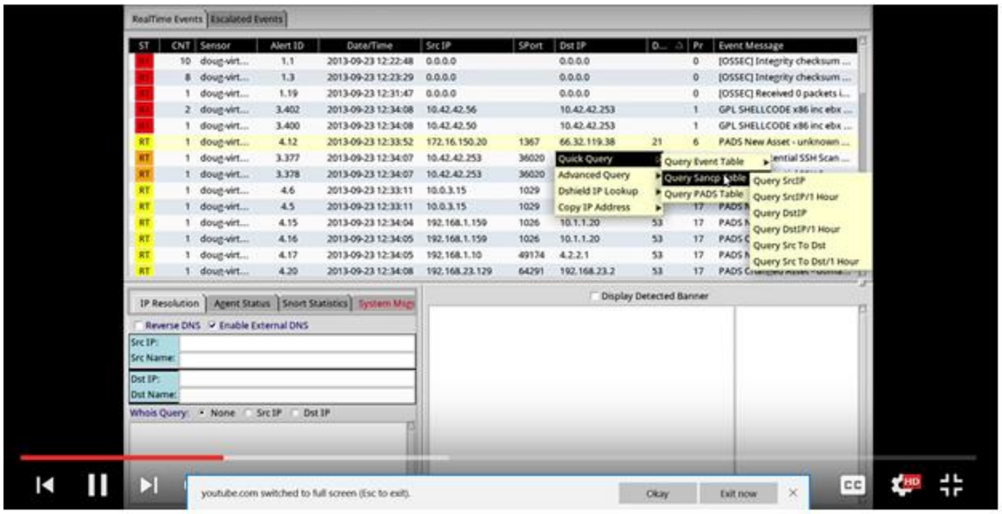
Project Name: Security Onion (Security Tool)
Network Intrusion Detection System.

What is Security Onion?
In simple words, it is a Digital Forensic Tool that makes Forensic Analysts life easy.

Plan: To implement Security Onion and analysis network traffic and find a way to remove file or network that compromise a system.

Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, Network Miner, and many other security tools. The easy-to-use Setup wizard allows to build an army of distributed sensors for enterprise in minutes.

The below picture shows the RealTime Events running in a system.



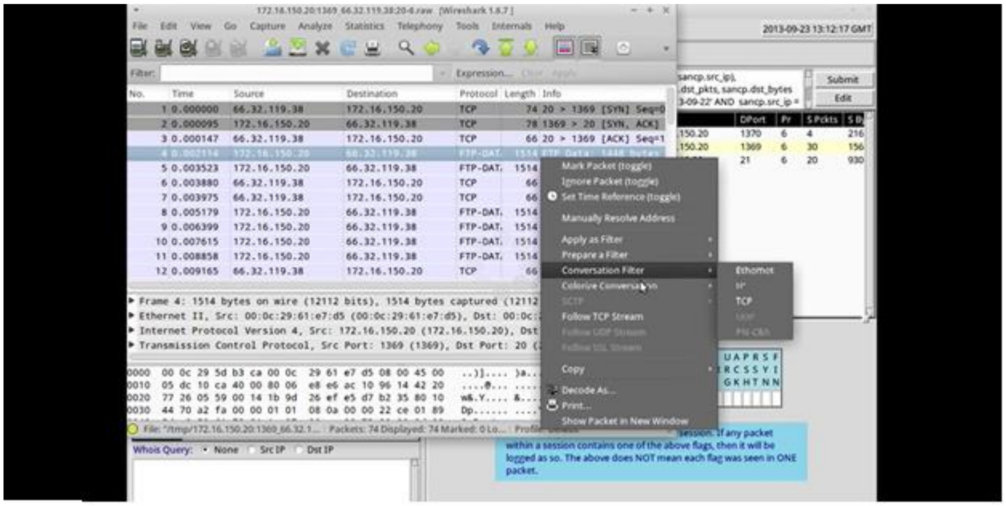
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	D...	Pr	Event Message
RT	10	doug-virt...	1.1	2013-09-23 12:22:48	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum ...
RT	8	doug-virt...	1.3	2013-09-23 12:23:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum ...
RT	1	doug-virt...	1.19	2013-09-23 12:31:47	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets i...
RT	2	doug-virt...	3.402	2013-09-23 12:34:08	10.42.42.56		10.42.42.253		1	GPL SHELLCODE x86 inc ebx ...
RT	1	doug-virt...	3.400	2013-09-23 12:34:08	10.42.42.50		10.42.42.253		1	GPL SHELLCODE x86 inc ebx ...
RT	1	doug-virt...	4.12	2013-09-23 12:33:52	172.16.150.20	1367	66.32.119.38	21	6	PADS New Asset - unknown ...
RT	1	doug-virt...	3.377	2013-09-23 12:34:07	10.42.42.253	36020				ential SSH Scan ...
RT	1	doug-virt...	3.378	2013-09-23 12:34:07	10.42.42.253	36020				
RT	1	doug-virt...	4.6	2013-09-23 12:33:11	10.0.3.15	1029			17	PADS
RT	1	doug-virt...	4.5	2013-09-23 12:33:11	10.0.3.15	1029			17	PADS N
RT	1	doug-virt...	4.15	2013-09-23 12:34:04	192.168.1.159	1026	10.1.1.20	53	17	PADS N
RT	1	doug-virt...	4.16	2013-09-23 12:34:05	192.168.1.159	1026	10.1.1.20	53	17	PADS C
RT	1	doug-virt...	4.17	2013-09-23 12:34:05	192.168.1.10	49174	4.2.2.1	53	17	PADS N
RT	1	doug-virt...	4.20	2013-09-23 12:34:08	192.168.23.129	64291	192.168.23.2	53	17	PADS Changed Asset - ...

☐ Reverse DNS ☑ Enable External DNS

Src IP:	
Src Name:	
Dst IP:	
Dst Name:	

Whois Query: ● None ○ Src IP ○ Dst IP

Then we analyzed the event using Wireshark to evaluate malware.



2013-09-23 13:12:17 GMT

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	66.32.119.38	172.16.150.20	TCP	74	20 > 1369 [SYN] Seq=0
2	0.000095	172.16.150.20	66.32.119.38	TCP	78	1369 > 20 [SYN, ACK]
3	0.000147	66.32.119.38	172.16.150.20	TCP	66	20 > 1369 [ACK] Seq=1
4	0.002114	172.16.150.20	66.32.119.38	FTP-DAT.	1514	FTP Data: 1448 bytes
5	0.003523	172.16.150.20	66.32.119.38	FTP-DAT.	1514	
6	0.003880	66.32.119.38	172.16.150.20	TCP	66	
7	0.003975	66.32.119.38	172.16.150.20	TCP	66	
8	0.005179	172.16.150.20	66.32.119.38	FTP-DAT.	1514	
9	0.006399	172.16.150.20	66.32.119.38	FTP-DAT.	1514	
10	0.007615	172.16.150.20	66.32.119.38	FTP-DAT.	1514	
11	0.008858	172.16.150.20	66.32.119.38	FTP-DAT.	1514	
12	0.009165	66.32.119.38	172.16.150.20	TCP	66	

```
▶ Frame 4: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112
▶ Ethernet II, Src: 00:0c:29:61:e7:d5 (00:0c:29:61:e7:d5), Dst: 00:0c:
▶ Internet Protocol Version 4, Src: 172.16.150.20 (172.16.150.20), Dst
▶ Transmission Control Protocol, Src Port: 1369 (1369), Dst Port: 20 (

0000  00 0c 29 5d b3 ca 00 0c  29 61 e7 d5 08 00 45 00   ..)]....  )a..
0010  05 dc 10 ca 40 00 80 06  e8 e6 ac 10 96 14 42 20   ....@...  ....
0020  77 26 05 59 00 14 1b 9d  26 ef e5 d7 b2 35 80 10   w&.Y....  &...
0030  44 70 a2 fa 00 00 01 01  08 0a 00 00 22 ce 01 89   Dp......  ....
```

File: "/tmp/172.16.150.20:1369_66.32.1... Packets: 74 Displayed: 74 Marked: 0 Lo... Profile: Default

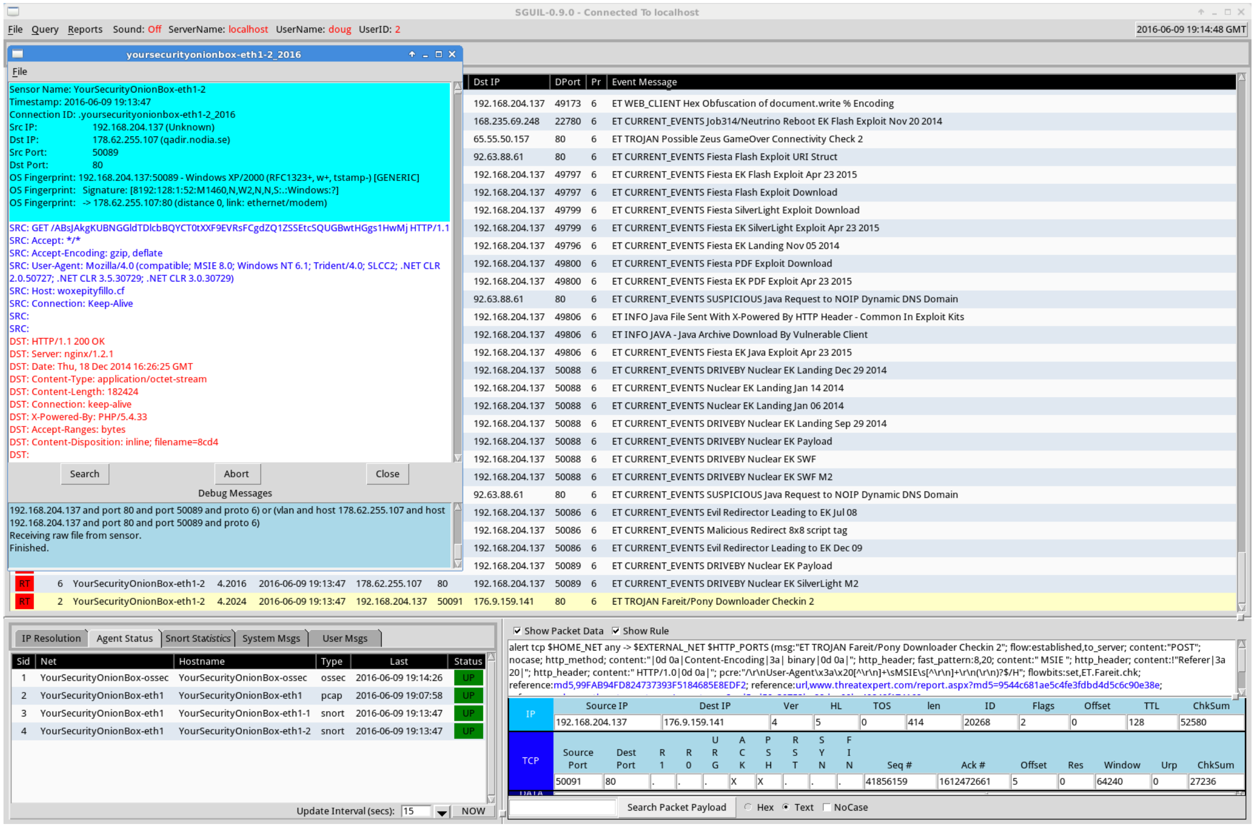
sancp.src_ip), dst_pkts, sancp.dst_bytes 3-09-22' AND sancp.src_ip =

	DPort	Pr	S Pckts	S B
150.20	1370	6	4	216
150.20	1369	6	30	156
	21	6	20	930

session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.

Whois Query: ● None ○ Src IP ○ Dst IP

With the help of Sguil(Default tool in Security Onion) all the packets were visible in multiple screens in one window and this helps to investigate on the raw data i.e binary file of the suspicious network.



Sound: Off ServerName: localhost UserName: doug UserID: 2 2016-06-09 19:14:48 GMT

```
Sensor Name: YourSecurityOnionBox-eth1-2
Timestamp: 2016-06-09 19:13:47
Connection ID: .yoursecurityonionbox-eth1-2_2016
Src IP:          192.168.204.137 (Unknown)
Dst IP:          178.62.255.107 (qadir.nodia.se)
Src Port:        50089
Dst Port:        80
OS Fingerprint: 192.168.204.137:50089 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W2,N,N,S:.:Windows:?]
OS Fingerprint:   -> 178.62.255.107:80 (distance 0, link: ethernet/modem)

SRC: GET /ABsJAkgKUBNGGldTDlcbBQYCT0tXXF9EVRsFCgdZQ1ZSSEtcSQUGBwtHGgs1HwMj HTTP/1.1
SRC: Accept: */*
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
SRC: Host: woxepityfillo.cf
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx/1.2.1
DST: Date: Thu, 18 Dec 2014 16:26:25 GMT
DST: Content-Type: application/octet-stream
DST: Content-Length: 182424
DST: Connection: keep-alive
DST: X-Powered-By: PHP/5.4.33
DST: Accept-Ranges: bytes
DST: Content-Disposition: inline; filename=8cd4
DST:
```

Debug Messages

```
192.168.204.137 and port 80 and port 50089 and proto 6) or (vlan and host 178.62.255.107 and host
192.168.204.137 and port 80 and port 50089 and proto 6)
Receiving raw file from sensor.
Finished.
```

							Dst IP	DPort	Pr	Event Message
							192.168.204.137	49173	6	ET WEB_CLIENT Hex Obfuscation of document.write % Encoding
							168.235.69.248	22780	6	ET CURRENT_EVENTS Job314/Neutrino Reboot EK Flash Exploit Nov 20 2014
							65.55.50.157	80	6	ET TROJAN Possible Zeus GameOver Connectivity Check 2
							92.63.88.61	80	6	ET CURRENT_EVENTS Fiesta Flash Exploit URI Struct
							192.168.204.137	49797	6	ET CURRENT_EVENTS Fiesta EK Flash Exploit Apr 23 2015
							192.168.204.137	49797	6	ET CURRENT_EVENTS Fiesta Flash Exploit Download
							192.168.204.137	49799	6	ET CURRENT_EVENTS Fiesta SilverLight Exploit Download
							192.168.204.137	49799	6	ET CURRENT_EVENTS Fiesta EK SilverLight Exploit Apr 23 2015
							192.168.204.137	49796	6	ET CURRENT_EVENTS Fiesta EK Landing Nov 05 2014
							192.168.204.137	49800	6	ET CURRENT_EVENTS Fiesta PDF Exploit Download
							192.168.204.137	49800	6	ET CURRENT_EVENTS Fiesta EK PDF Exploit Apr 23 2015
							92.63.88.61	80	6	ET CURRENT_EVENTS SUSPICIOUS Java Request to NOIP Dynamic DNS Domain
							192.168.204.137	49806	6	ET INFO Java File Sent With X-Powered By HTTP Header - Common In Exploit Kits
							192.168.204.137	49806	6	ET INFO JAVA - Java Archive Download By Vulnerable Client
							192.168.204.137	49806	6	ET CURRENT_EVENTS Fiesta EK Java Exploit Apr 23 2015
							192.168.204.137	50088	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK Landing Dec 29 2014
							192.168.204.137	50088	6	ET CURRENT_EVENTS Nuclear EK Landing Jan 14 2014
							192.168.204.137	50088	6	ET CURRENT_EVENTS Nuclear EK Landing Jan 06 2014
							192.168.204.137	50088	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK Landing Sep 29 2014
							192.168.204.137	50088	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK Payload
							192.168.204.137	50088	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK SWF
							192.168.204.137	50088	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK SWF M2
							92.63.88.61	80	6	ET CURRENT_EVENTS SUSPICIOUS Java Request to NOIP Dynamic DNS Domain
							192.168.204.137	50086	6	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 08
							192.168.204.137	50086	6	ET CURRENT_EVENTS Malicious Redirect 8x8 script tag
							192.168.204.137	50086	6	ET CURRENT_EVENTS Evil Redirector Leading to EK Dec 09
							192.168.204.137	50089	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK Payload
RT	6	YourSecurityOnionBox-eth1-2	4.2016	2016-06-09 19:13:47	178.62.255.107	80	192.168.204.137	50089	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK SilverLight M2
RT	2	YourSecurityOnionBox-eth1-2	4.2024	2016-06-09 19:13:47	192.168.204.137	50091	176.9.159.141	80	6	ET TROJAN Fareit/Pony Downloader Checkin 2

Sid	Net	Hostname	Type	Last	Status
1	YourSecurityOnionBox-ossec	YourSecurityOnionBox-ossec	ossec	2016-06-09 19:14:26	UP
2	YourSecurityOnionBox-eth1	YourSecurityOnionBox-eth1	pcap	2016-06-09 19:07:58	UP
3	YourSecurityOnionBox-eth1	YourSecurityOnionBox-eth1-1	snort	2016-06-09 19:13:47	UP
4	YourSecurityOnionBox-eth1	YourSecurityOnionBox-eth1-2	snort	2016-06-09 19:13:47	UP

Update Interval (secs): 15 NOW

☑ Show Packet Data ☑ Show Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fareit/Pony Downloader Checkin 2"; flow:established,to_server; content:"POST";
nocase; http_method; content:"|0d 0a|Content-Encoding|3a| binary|0d 0a|"; http_header; fast_pattern:8,20; content:" MSIE "; http_header; content:!"Referer|3a
20|"; http_header; content:" HTTP/1.0|0d 0a|"; pcre:"/\r\nUser-Agent\x3a\x20[^\r\n]+\sMSIE\s[^\r\n]+\r\n(\r\n)?$/H"; flowbits:set,ET.Fareit.chk;
reference:md5,99FAB94FD824737393F5184685E8EDF2; reference:url,www.threatexpert.com/report.aspx?md5=9544c681ae5c4fe3fdbd4d5c6c90e38e;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.204.137	176.9.159.141	4	5	0	414	20268	2	0	128	52580

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	50091	80	.	.	.	X	X	.	.	.	41856159	1612472661	5	0	64240	0	27236

○ Hex ● Text □ NoCase

All of the above data is collected by virtualization aka installing various operating system under one host operating system. We downloaded, Kali Linux, Ubuntu 64bits, Metasploitable, Wireshark, Security Onion as virtual OS in one host Windows OS. This type of system is known as standalone system.

We also wanted to find a way to mitigate the risk of incoming suspicious network but due to restriction of time and poor Internet connection we could not accomplish our goal. But we, will continue our work after Bitcamp also.

Thank You.

Team Members,
Khushali Dalal (University of Maryland)
Dhairya Patel(Florida International University)