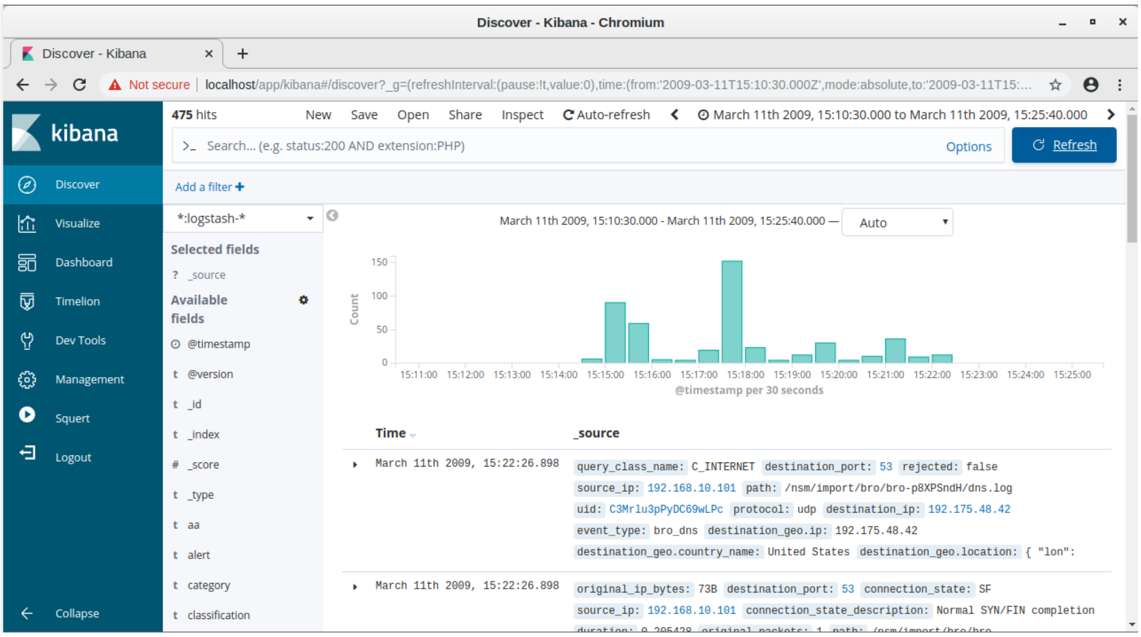
/**

Jako trzeci do analizy wybrałem i zaimportowałem plik `example.com-1.pcap` .

`sudo so-import-pcap example.com-1.pcap` Ponownie zacząłem od Kibany i Squerta.

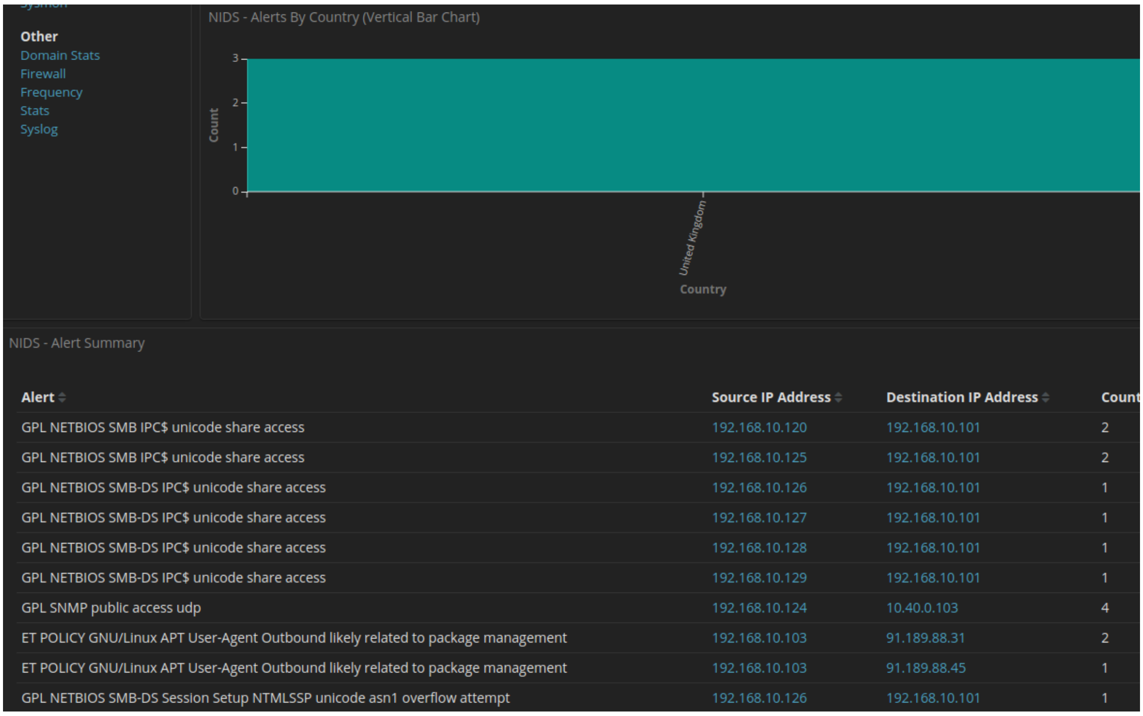
Widok zaimportowanego ruchu w Kibanie



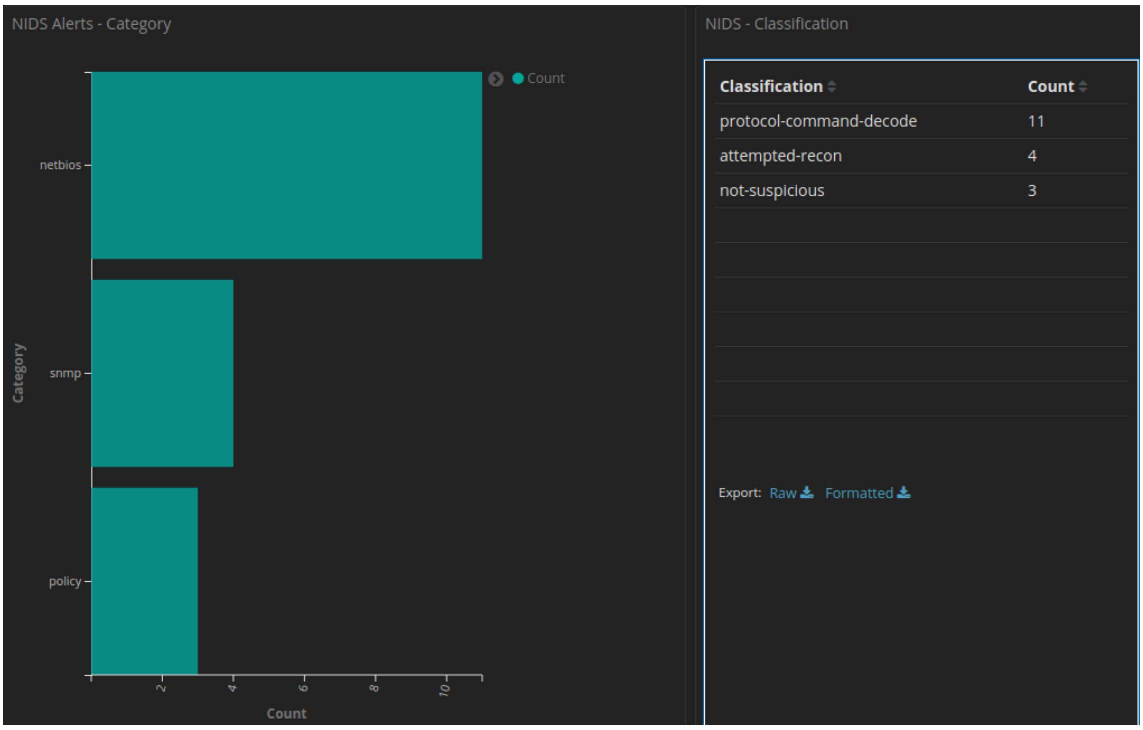
```
March 11th 2009, 15:22:26.898   query_class_name: C_INTERNET destination_port: 53 rejected: false
                                source_ip: 192.168.10.101 path: /nsm/import/bro/bro-p8XPSndH/dns.log
                                uid: C3Mrlu3pPyDC69wLPc protocol: udp destination_ip: 192.175.48.42
                                event_type: bro_dns destination_geo.ip: 192.175.48.42
                                destination_geo.country_name: United States destination_geo.location: { "lon":

March 11th 2009, 15:22:26.898   original_ip_bytes: 73B destination_port: 53 connection_state: SF
                                source_ip: 192.168.10.101 connection_state_description: Normal SYN/FIN completion
                                duration: 0.205428 original_packets: 1 path: /nsm/import/bro/bro
```

Podsumowania alertów NIDS oraz ich podział na poszczególne kategorie



Alert	Source IP Address	Destination IP Address	Count
GPL NETBIOS SMB IPC$ unicode share access	192.168.10.120	192.168.10.101	2
GPL NETBIOS SMB IPC$ unicode share access	192.168.10.125	192.168.10.101	2
GPL NETBIOS SMB-DS IPC$ unicode share access	192.168.10.126	192.168.10.101	1
GPL NETBIOS SMB-DS IPC$ unicode share access	192.168.10.127	192.168.10.101	1
GPL NETBIOS SMB-DS IPC$ unicode share access	192.168.10.128	192.168.10.101	1
GPL NETBIOS SMB-DS IPC$ unicode share access	192.168.10.129	192.168.10.101	1
GPL SNMP public access udp	192.168.10.124	10.40.0.103	4
ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	192.168.10.103	91.189.88.31	2
ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	192.168.10.103	91.189.88.45	1
GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt	192.168.10.126	192.168.10.101	1

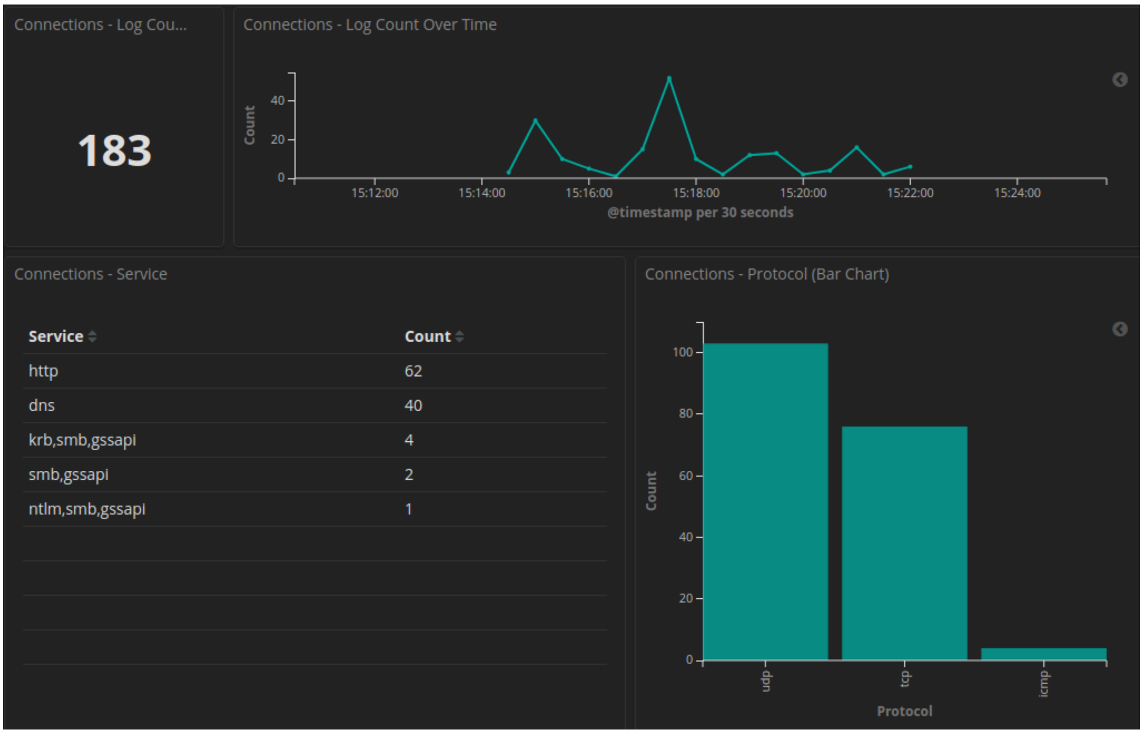


NIDS - Classification

Classification	Count
protocol-command-decode	11
attempted-recon	4
not-suspicious	3

Export: Raw Formatted

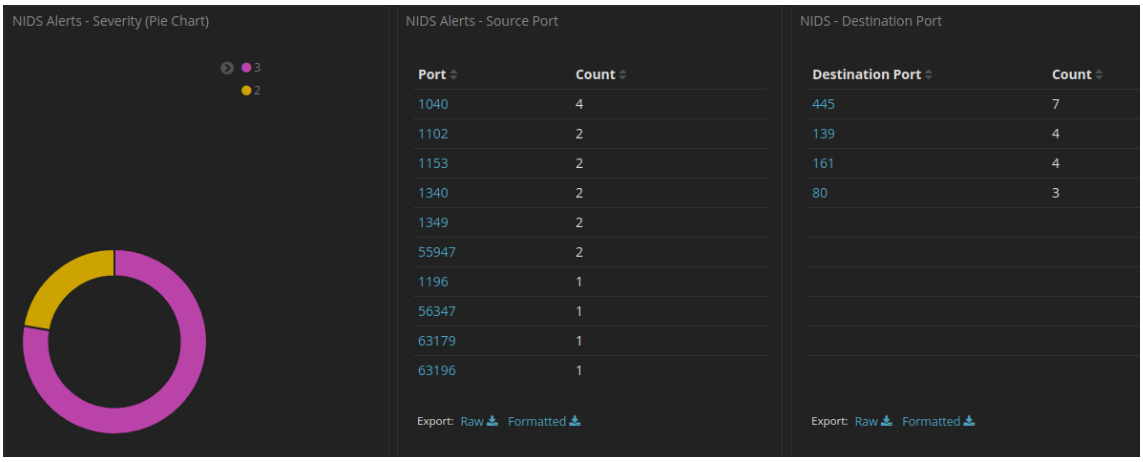
Usługi działające podczas ataku oraz wykorzystywane protokoły



Connections - Service

Service	Count
http	62
dns	40
krb,smb,gssapi	4
smb,gssapi	2
ntlm,smb,gssapi	1

Porty na których odbywała się komunikacja, oraz dodatkowe informacje na ich temat



NIDS Alerts - Severity (Pie Chart)

NIDS Alerts - Source Port

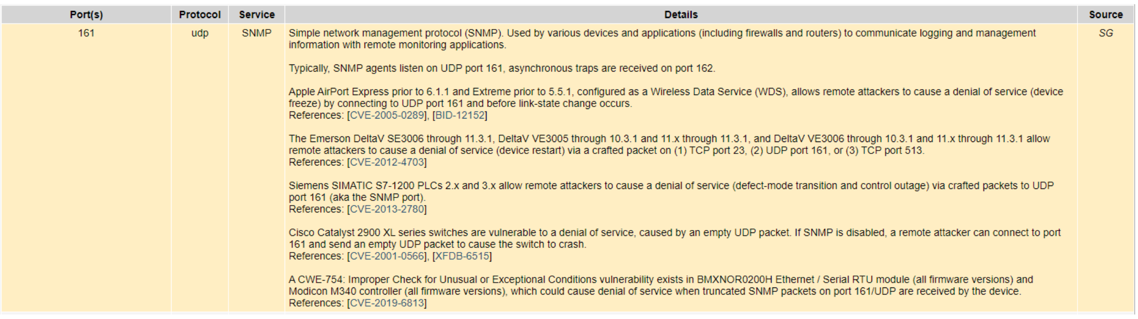
Port	Count
1040	4
1102	2
1153	2
1340	2
1349	2
55947	2
1196	1
56347	1
63179	1
63196	1

Export: Raw Formatted

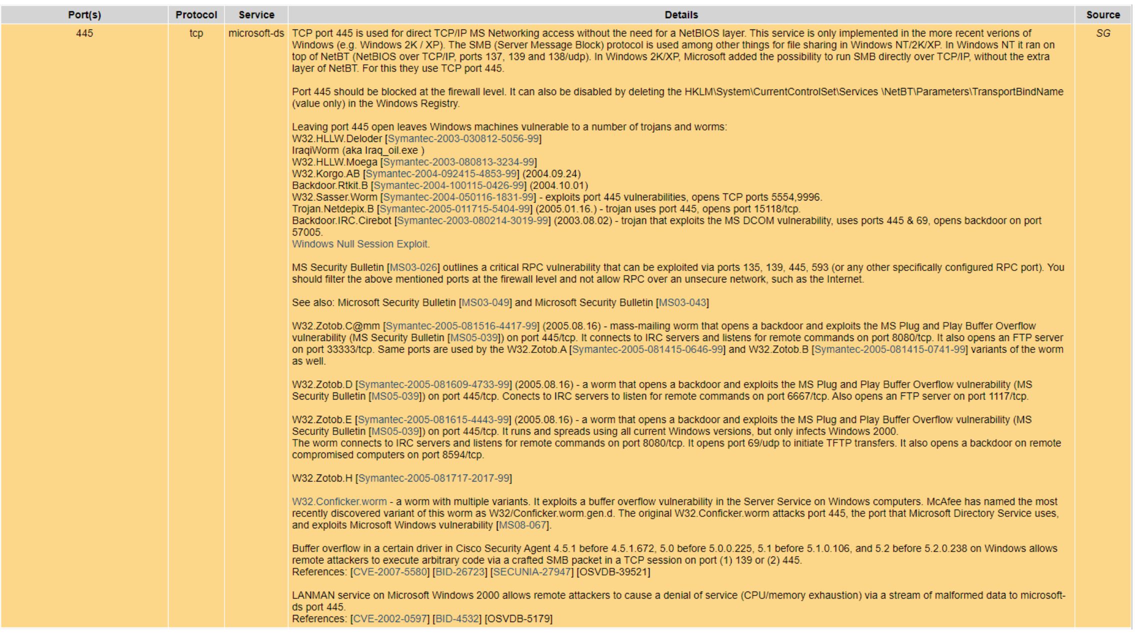
NIDS - Destination Port

Destination Port	Count
445	7
139	4
161	4
80	3

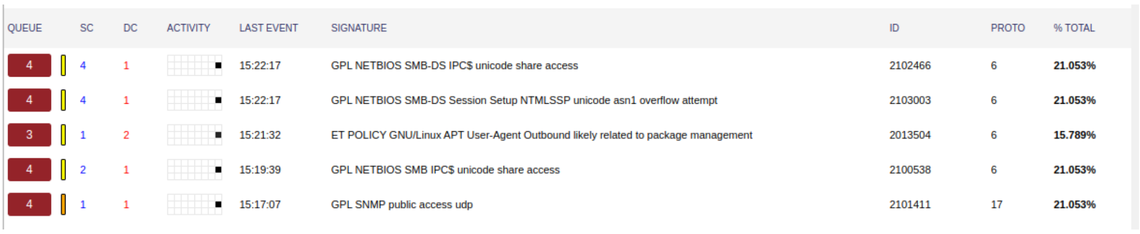
Export: Raw Formatted



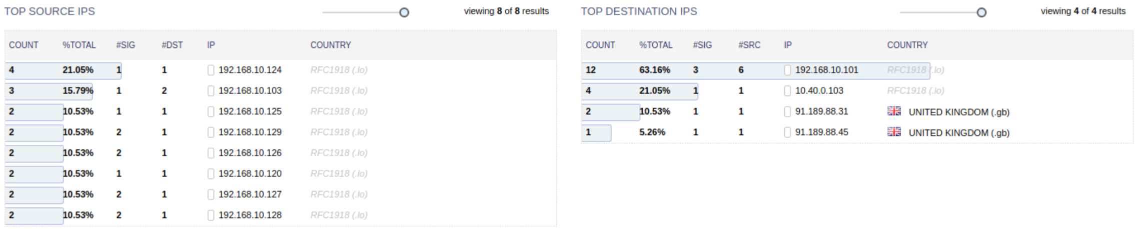
Port(s)	Protocol	Service	Details	Source
161	udp	SNMP	Simple network management protocol (SNMP). Used by various devices and applications (including firewalls and routers) to communicate logging and management information with remote monitoring applications. Typically, SNMP agents listen on UDP port 161, asynchronous traps are received on port 162. Apple AirPort Express prior to 6.1.1 and Extreme prior to 5.5.1, configured as a Wireless Data Service (WDS), allows remote attackers to cause a denial of service (device freeze) by connecting to UDP port 161 and before link-state change occurs. References: [CVE-2005-0289], [BID-12152] The Emerson DeltaV SE3006 through 11.3.1, DeltaV VE3005 through 10.3.1 and 11.x through 11.3.1, and DeltaV VE3006 through 10.3.1 and 11.x through 11.3.1 allow remote attackers to cause a denial of service (device restart) via a crafted packet on (1) TCP port 23, (2) UDP port 161, or (3) TCP port 513. References: [CVE-2012-4703] Siemens SIMATIC S7-1200 PLCs 2.x and 3.x allow remote attackers to cause a denial of service (defect-mode transition and control outage) via crafted packets to UDP port 161 (aka the SNMP port). References: [CVE-2013-2780] Cisco Catalyst 2900 XL series switches are vulnerable to a denial of service, caused by an empty UDP packet. If SNMP is disabled, a remote attacker can connect to port 161 and send an empty UDP packet to cause the switch to crash. References: [CVE-2001-0566], [XFDB-6515] A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in BMXNOR0200H Ethernet / Serial RTU module (all firmware versions) and Modicon M340 controller (all firmware versions), which could cause denial of service when truncated SNMP packets on port 161/UDP are received by the device. References: [CVE-2019-6813]	*SG*



Port(s)	Protocol	Service	Details	Source
445	tcp	microsoft-ds	TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. This service is only implemented in the more recent verions of Windows (e.g. Windows 2K / XP). The SMB (Server Message Block) protocol is used among other things for file sharing in Windows NT/2K/XP. In Windows NT it ran on top of NetBT (NetBIOS over TCP/IP, ports 137, 139 and 138/udp). In Windows 2K/XP, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra layer of NetBT. For this they use TCP port 445. Port 445 should be blocked at the firewall level. It can also be disabled by deleting the HKLM\System\CurrentControlSet\Services \NetBT\Parameters\TransportBindName (value only) in the Windows Registry. Leaving port 445 open leaves Windows machines vulnerable to a number of trojans and worms: W32.HLLW.Deloder [Symantec-2003-030812-5056-99] IraqiWorm (aka Iraq_oil.exe) W32.HLLW.Moega [Symantec-2003-080813-3234-99] W32.Korgo.AB [Symantec-2004-092415-4853-99] (2004.09.24) Backdoor.Rtkit.B [Symantec-2004-100115-0426-99] (2004.10.01) W32.Sasser.Worm [Symantec-2004-050116-1831-99] - exploits port 445 vulnerabilities, opens TCP ports 5554,9996. Trojan.Netdepix.B [Symantec-2005-011715-5404-99] (2005.01.16.) - trojan uses port 445, opens port 15118/tcp. Backdoor.IRC.Cirebot [Symantec-2003-080214-3019-99] (2003.08.02) - trojan that exploits the MS DCOM vulnerability, uses ports 445 & 69, opens backdoor on port 57005. Windows Null Session Exploit. MS Security Bulletin [MS03-026] outlines a critical RPC vulnerability that can be exploited via ports 135, 139, 445, 593 (or any other specifically configured RPC port). You should filter the above mentioned ports at the firewall level and not allow RPC over an unsecure network, such as the Internet. See also: Microsoft Security Bulletin [MS03-049] and Microsoft Security Bulletin [MS03-043] W32.Zotob.C@mm [Symantec-2005-081516-4417-99] (2005.08.16) - mass-mailing worm that opens a backdoor and exploits the MS Plug and Play Buffer Overflow vulnerability (MS Security Bulletin [MS05-039]) on port 445/tcp. It connects to IRC servers and listens for remote commands on port 8080/tcp. It also opens an FTP server on port 33333/tcp. Same ports are used by the W32.Zotob.A [Symantec-2005-081415-0646-99] and W32.Zotob.B [Symantec-2005-081415-0741-99] variants of the worm as well. W32.Zotob.D [Symantec-2005-081609-4733-99] (2005.08.16) - a worm that opens a backdoor and exploits the MS Plug and Play Buffer Overflow vulnerability (MS Security Bulletin [MS05-039]) on port 445/tcp. Conects to IRC servers to listen for remote commands on port 6667/tcp. Also opens an FTP server on port 1117/tcp. W32.Zotob.E [Symantec-2005-081615-4443-99] (2005.08.16) - a worm that opens a backdoor and exploits the MS Plug and Play Buffer Overflow vulnerability (MS Security Bulletin [MS05-039]) on port 445/tcp. It runs and spreads using all current Windows versions, but only infects Windows 2000. The worm connects to IRC servers and listens for remote commands on port 8080/tcp. It opens port 69/udp to initiate TFTP transfers. It also opens a backdoor on remote compromised computers on port 8594/tcp. W32.Zotob.H [Symantec-2005-081717-2017-99] W32.Conficker.worm - a worm with multiple variants. It exploits a buffer overflow vulnerability in the Server Service on Windows computers. McAfee has named the most recently discovered variant of this worm as W32/Conficker.worm.gen.d. The original W32.Conficker.worm attacks port 445, the port that Microsoft Directory Service uses, and exploits Microsoft Windows vulnerability [MS08-067]. Buffer overflow in a certain driver in Cisco Security Agent 4.5.1 before 4.5.1.672, 5.0 before 5.0.0.225, 5.1 before 5.1.0.106, and 5.2 before 5.2.0.238 on Windows allows remote attackers to execute arbitrary code via a crafted SMB packet in a TCP session on port (1) 139 or (2) 445. References: [CVE-2007-5580] [BID-26723] [SECUNIA-27947] [OSVDB-39521] LANMAN service on Microsoft Windows 2000 allows remote attackers to cause a denial of service (CPU/memory exhaustion) via a stream of malformed data to microsoft-ds port 445. References: [CVE-2002-0597] [BID-4532] [OSVDB-5179]	*SG*



QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
4	4	1	■	15:22:17	GPL NETBIOS SMB-DS IPC$ unicode share access	2102466	6	**21.053%**
4	4	1	■	15:22:17	GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt	2103003	6	**21.053%**
3	1	2	■	15:21:32	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	2013504	6	**15.789%**
4	2	1	■	15:19:39	GPL NETBIOS SMB IPC$ unicode share access	2100538	6	**21.053%**
4	1	1	■	15:17:07	GPL SNMP public access udp	2101411	17	**21.053%**



TOP SOURCE IPS

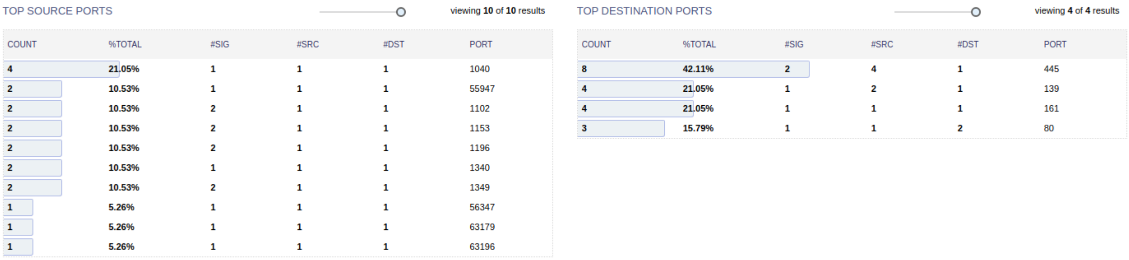
viewing **8** of **8** results

COUNT	%TOTAL	#SIG	#DST	IP	COUNTRY
4	**21.05%**	**1**	**1**	192.168.10.124	*RFC1918 (.lo)*
3	**15.79%**	**1**	**2**	192.168.10.103	*RFC1918 (.lo)*
2	**10.53%**	**1**	**1**	192.168.10.125	*RFC1918 (.lo)*
2	**10.53%**	**2**	**1**	192.168.10.129	*RFC1918 (.lo)*
2	**10.53%**	**2**	**1**	192.168.10.126	*RFC1918 (.lo)*
2	**10.53%**	**1**	**1**	192.168.10.120	*RFC1918 (.lo)*
2	**10.53%**	**2**	**1**	192.168.10.127	*RFC1918 (.lo)*
2	**10.53%**	**2**	**1**	192.168.10.128	*RFC1918 (.lo)*

TOP DESTINATION IPS

viewing **4** of **4** results

COUNT	%TOTAL	#SIG	#SRC	IP	COUNTRY
12	**63.16%**	**3**	**6**	192.168.10.101	*RFC1918 (.lo)*
4	**21.05%**	**1**	**1**	10.40.0.103	*RFC1918 (.lo)*
2	**10.53%**	**1**	**1**	91.189.88.31	UNITED KINGDOM (.gb)
1	**5.26%**	**1**	**1**	91.189.88.45	UNITED KINGDOM (.gb)



TOP SOURCE PORTS

viewing **10** of **10** results

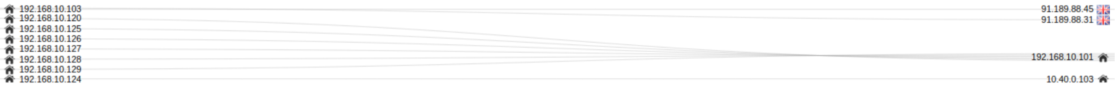
COUNT	%TOTAL	#SIG	#SRC	#DST	PORT
4	**21.05%**	**1**	**1**	**1**	1040
2	**10.53%**	**1**	**1**	**1**	55947
2	**10.53%**	**2**	**1**	**1**	1102
2	**10.53%**	**2**	**1**	**1**	1153
2	**10.53%**	**2**	**1**	**1**	1196
2	**10.53%**	**1**	**1**	**1**	1340
2	**10.53%**	**2**	**1**	**1**	1349
1	**5.26%**	**1**	**1**	**1**	56347
1	**5.26%**	**1**	**1**	**1**	63179
1	**5.26%**	**1**	**1**	**1**	63196

TOP DESTINATION PORTS

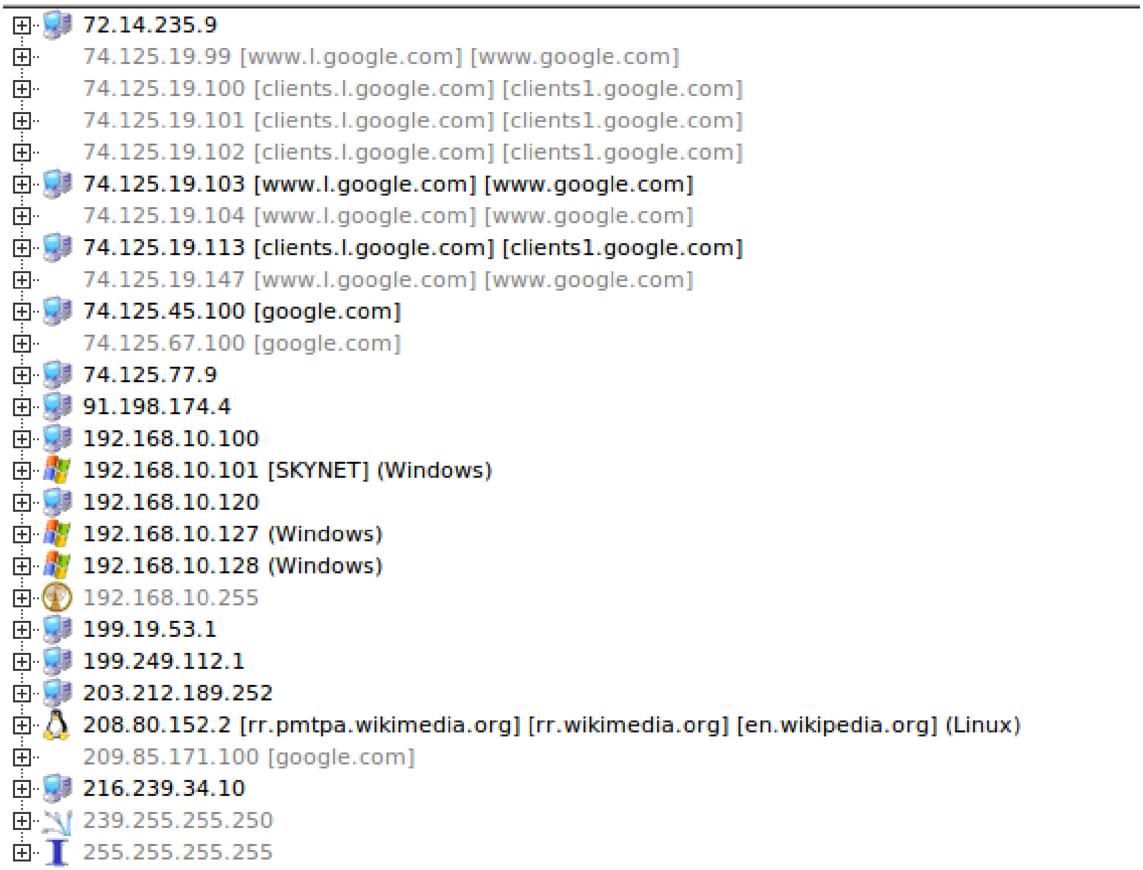
viewing **4** of **4** results

COUNT	%TOTAL	#SIG	#SRC	#DST	PORT
8	**42.11%**	**2**	**4**	**1**	445
4	**21.05%**	**1**	**2**	**1**	139
4	**21.05%**	**1**	**1**	**1**	161
3	**15.79%**	**1**	**1**	**2**	80

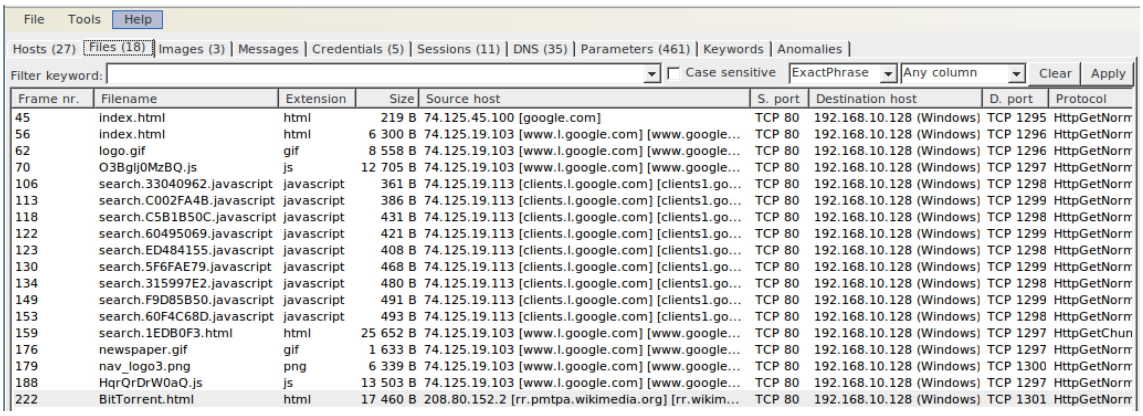
Z tego diagramu wynika że nasz host komunikował się z innymi urządzeniami w sieci wewnętrznej a także zewnętrzynym adresem IP pochodzącym z UK



W Programie Network Miner uzyskałem informację o hostach, a wyodrębnione pliki z ruchu sieciowego



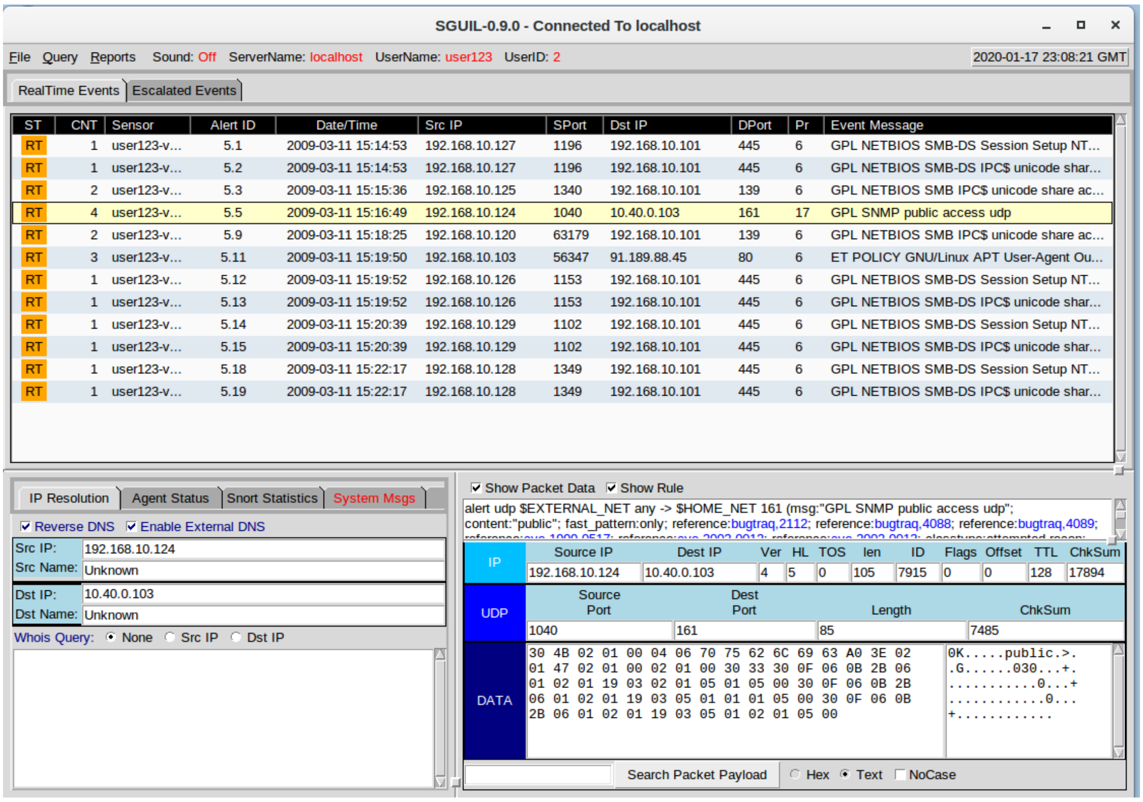
```
72.14.235.9
74.125.19.99 [www.l.google.com] [www.google.com]
74.125.19.100 [clients.l.google.com] [clients1.google.com]
74.125.19.101 [clients.l.google.com] [clients1.google.com]
74.125.19.102 [clients.l.google.com] [clients1.google.com]
74.125.19.103 [www.l.google.com] [www.google.com]
74.125.19.104 [www.l.google.com] [www.google.com]
74.125.19.113 [clients.l.google.com] [clients1.google.com]
74.125.19.147 [www.l.google.com] [www.google.com]
74.125.45.100 [google.com]
74.125.67.100 [google.com]
74.125.77.9
91.198.174.4
192.168.10.100
192.168.10.101 [SKYNET] (Windows)
192.168.10.120
192.168.10.127 (Windows)
192.168.10.128 (Windows)
192.168.10.255
199.19.53.1
199.249.112.1
203.212.189.252
208.80.152.2 [rr.pmtpa.wikimedia.org] [rr.wikimedia.org] [en.wikipedia.org] (Linux)
209.85.171.100 [google.com]
216.239.34.10
239.255.255.250
255.255.255.255
```



File
Tools
Help
Hosts (27) | Files (18) | Images (3) | Messages | Credentials (5) | Sessions (11) | DNS (35) | Parameters (461) | Keywords | Anomalies
Filter keyword:
□ Case sensitive
ExactPhrase
Any column
Clear
Apply

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol
45	index.html	html	219 B	74.125.45.100 [google.com]	TCP 80	192.168.10.128 (Windows)	TCP 1295	HttpGetNorm
56	index.html	html	6 300 B	74.125.19.103 [www.l.google.com] [www.google...	TCP 80	192.168.10.128 (Windows)	TCP 1296	HttpGetNorm
62	logo.gif	gif	8 558 B	74.125.19.103 [www.l.google.com] [www.google...	TCP 80	192.168.10.128 (Windows)	TCP 1296	HttpGetNorm
70	O3Bglj0MzBQ.js	js	12 705 B	74.125.19.103 [www.l.google.com] [www.google...	TCP 80	192.168.10.128 (Windows)	TCP 1297	HttpGetNorm
106	search.33040962.javascript	javascript	361 B	74.125.19.113 [clients.l.google.com] [clients1.go...	TCP 80	192.168.10.128 (Windows)	TCP 1298	HttpGetNorm
113	search.C002FA4B.javascript	javascript	386 B	74.125.19.113 [clients.l.google.com] [clients1.go...	TCP 80	192.168.10.128 (Windows)	TCP 1299	HttpGetNorm
118	search.C5B1B50C.javascript	javascript	431 B	74.125.19.113 [clients.l.google.com] [clients1.go...	TCP 80	192.168.10.128 (Windows)	TCP 1298	HttpGetNorm
122	search.60495069.javascript	javascript	421 B	74.125.19.113 [clients.l.google.com] [clients1.go...	TCP 80	192.168.10.128 (Windows)	TCP 1299	HttpGetNorm
123	search.ED484155.javascript	javascript	408 B	74.125.19.113 [clients.l.google.com] [clients1.go...	TCP 80	192.168.10.128 (Windows)	TCP 1298	HttpGetNorm
130	search.5F6FAE79.javascript	javascript	468 B	74.125.19.113 [clients.l.google.com] [clients1.go...	TCP 80	192.168.10.128 (Windows)	TCP 1299	HttpGetNorm
134	search.315997E2.javascript	javascript	480 B	74.125.19.113 [clients.l.google.com] [clients1.go...	TCP 80	192.168.10.128 (Windows)	TCP 1298	HttpGetNorm
149	search.F9D85B50.javascript	javascript	491 B	74.125.19.113 [clients.l.google.com] [clients1.go...	TCP 80	192.168.10.128 (Windows)	TCP 1299	HttpGetNorm
153	search.60F4C68D.javascript	javascript	493 B	74.125.19.113 [clients.l.google.com] [clients1.go...	TCP 80	192.168.10.128 (Windows)	TCP 1298	HttpGetNorm
159	search.1EDB0F3.html	html	25 652 B	74.125.19.103 [www.l.google.com] [www.google...	TCP 80	192.168.10.128 (Windows)	TCP 1297	HttpGetChun
176	newspaper.gif	gif	1 633 B	74.125.19.103 [www.l.google.com] [www.google...	TCP 80	192.168.10.128 (Windows)	TCP 1297	HttpGetNorm
179	nav_logo3.png	png	6 339 B	74.125.19.103 [www.l.google.com] [www.google...	TCP 80	192.168.10.128 (Windows)	TCP 1300	HttpGetNorm
188	HqrQrDrW0aQ.js	js	13 503 B	74.125.19.103 [www.l.google.com] [www.google...	TCP 80	192.168.10.128 (Windows)	TCP 1297	HttpGetNorm
222	BitTorrent.html	html	17 460 B	208.80.152.2 [rr.pmtpa.wikimedia.org] [rr.wikim...	TCP 80	192.168.10.128 (Windows)	TCP 1301	HttpGetNorm

Sprawdziłem także widok logów w programi Sguily


SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: user123 UserID: 2 2020-01-17 23:08:21 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	user123-v...	5.1	2009-03-11 15:14:53	192.168.10.127	1196	192.168.10.101	445	6	GPL NETBIOS SMB-DS Session Setup NT...
RT	1	user123-v...	5.2	2009-03-11 15:14:53	192.168.10.127	1196	192.168.10.101	445	6	GPL NETBIOS SMB-DS IPC$ unicode shar...
RT	2	user123-v...	5.3	2009-03-11 15:15:36	192.168.10.125	1340	192.168.10.101	139	6	GPL NETBIOS SMB IPC$ unicode share ac...
RT	4	user123-v...	5.5	2009-03-11 15:16:49	192.168.10.124	1040	10.40.0.103	161	17	GPL SNMP public access udp
RT	2	user123-v...	5.9	2009-03-11 15:18:25	192.168.10.120	63179	192.168.10.101	139	6	GPL NETBIOS SMB IPC$ unicode share ac...
RT	3	user123-v...	5.11	2009-03-11 15:19:50	192.168.10.103	56347	91.189.88.45	80	6	ET POLICY GNU/Linux APT User-Agent Ou...
RT	1	user123-v...	5.12	2009-03-11 15:19:52	192.168.10.126	1153	192.168.10.101	445	6	GPL NETBIOS SMB-DS Session Setup NT...
RT	1	user123-v...	5.13	2009-03-11 15:19:52	192.168.10.126	1153	192.168.10.101	445	6	GPL NETBIOS SMB-DS IPC$ unicode shar...
RT	1	user123-v...	5.14	2009-03-11 15:20:39	192.168.10.129	1102	192.168.10.101	445	6	GPL NETBIOS SMB-DS Session Setup NT...
RT	1	user123-v...	5.15	2009-03-11 15:20:39	192.168.10.129	1102	192.168.10.101	445	6	GPL NETBIOS SMB-DS IPC$ unicode shar...
RT	1	user123-v...	5.18	2009-03-11 15:22:17	192.168.10.128	1349	192.168.10.101	445	6	GPL NETBIOS SMB-DS Session Setup NT...
RT	1	user123-v...	5.19	2009-03-11 15:22:17	192.168.10.128	1349	192.168.10.101	445	6	GPL NETBIOS SMB-DS IPC$ unicode shar...

☑ Reverse DNS ☑ Enable External DNS

Src IP:	192.168.10.124
Src Name:	Unknown
Dst IP:	10.40.0.103
Dst Name:	Unknown

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"GPL SNMP public access udp";
content:"public"; fast_pattern:only; reference:bugtraq,2112; reference:bugtraq,4088; reference:bugtraq,4089;
reference:cve,1999-0517; reference:cve,2002-0012; reference:cve,2002-0013; classtype:attempted-recon;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.10.124	10.40.0.103	4	5	0	105	7915	0	0	128	17894

UDP	Source Port	Dest Port	Length	ChkSum
	1040	161	85	7485

DATA

```
30 4B 02 01 00 04 06 70 75 62 6C 69 63 A0 3E 02    0K.....public.>.
01 47 02 01 00 02 01 00 30 33 30 0F 06 0B 2B 06    .G......030...+.
01 02 01 19 03 02 01 05 01 05 00 30 0F 06 0B 2B    ...........0...+
06 01 02 01 19 03 05 01 01 01 05 00 30 0F 06 0B    ............0...
2B 06 01 02 01 19 03 05 01 02 01 05 00             +............
```

○ Hex ● Text □ NoCase

*/