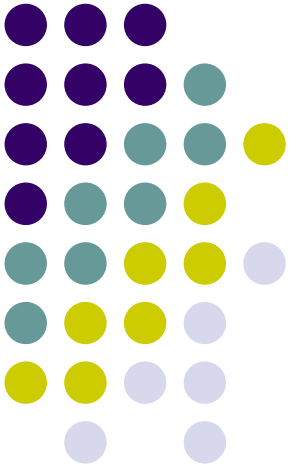
Otkrivanje upada

Intrusion Detection

Aco Dmitrović

SRCE

siječanj 2004.



Zahvala

- SANS Institute
- *SysAdmin, Audit, Networking and Security Institute*
- www.sans.org

- *Track 3* - Intrusion Detection In-Depth

Predznanje

- Potrebno je dobro poznavanje TCP/IP grupe protokola
- Poznavanje mreže (CCNA)

- Richard Stevens: TCP/IP Illustrated I,II,III
- IBM: TCP/IP Tutorial and Technical Overview

Učenje

- Upoznati prijetnje
- Upoznati protivnika
  - White Hats, Black Hats, Scriptie Kidz
- Biti otvoren, neprestano učiti

Priprema napada

- **I faza: izviđanje**
  - Mapiranje mreže
  - Skeniranje hostova
    - Detekcija OS-a
    - Aktivni servisi
    - Verzije aplikacija
  - Otkrivanje slabih točaka
  - Izbor vrste napada, alata

Ispitivanje

- Podražaj – odgovor
  - (*stimulus – response)*

- Besplatni alati
  - nmap http://www.insecure.org/nmap
  - Nessus http://www.nessus.org/
  - hping http://www.hping.org/

OS fingerprintig

```
regoc:~/skripte# nmap -nO host.domain.hr

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-27 16:52 CET
Interesting ports on 161.53.xxx.3:
PORT     STATE    SERVICE
 21/tcp   open     ftp
 22/tcp   open     ssh
 23/tcp   open     telnet
 25/tcp   open     smtp
 53/tcp   open     domain
 80/tcp   open     http
110/tcp   open     pop-3
143/tcp   open     imap
Running: Linux 2.4.X
OS details: Linux 2.4.20 - 2.4.21 w/grsecurity.org patch
Uptime 22.176 days (since Fri Dec  5 12:39:00 2003)
```

Napad

- **II faza: napad**
  - Uskraćivanje usluga (DoS)
    - Na pr. preplavljivanje (*flooding*)
  - Preuzimanje računala
    - Npr. napad prepisivanjem spremnika
    - Instalacija *rootkita* (skrivanje procesa, datoteka)
    - Instalacija servisa (npr. IRC proxy, anonymous FTP)
  - Automatski napadi (crvi)

Primjer

- Prva skeniranja porta 1433 - Dec. 2000.

- **Date: Tue Nov 20 2001** - 08:54:18 CST

We saw a scan come in looking for systems answering on 1433, and immediately saw several systems start scanning out for other systems answering on 1433 - worm behavior? Has anyone else seen this?

Nov 20 09:38:19 x.x.92.228:2884 -> x.x.90.70:**1433** SYN ******S*

Odgovor

From: Arthur Donkers (*A.Donkers reseau.nl*)

Date: Tue Nov 20 2001 - 10:40:02 CST

This is an exploit for a default MS SQL installation. If you check your trace it **calls xp_cmdshell** (which enables anyone to run a dos command directly from MSSQL, much like 'system' under Unix). It **ftp's a trojan** from foo.com (dnsservice.exe) and executes it. (after glancing through your log).

You probably have a **default MSSQL 7 installation with TCPIP connectivity that has an sa account with an empty password.**

Better disconnect and clean up

Trace

[**] MS-SQL xp_cmdshell - program execution [**]

11/20-08:01:48.923210 x.x.92.228:3348 -> x.x.200.115:1433
TCP TTL:127 TOS:0x0 ID:45385 IpLen:20 DgmLen:972 DF
AP Seq: 0x318F3D1 Ack: 0x1E5807AD Win: 0x2098 TcpLen: 20
03 01 03 A4 00 00 01 00 0A 00 73 00 70 00 5F 00 .....s.p._.
70 00 72 00 65 00 70 00 61 00 72 00 65 00 00 00 p.r.e.p.a.r.e...
00 01 26 04 00 00 00 63 00 00 00 00 FF FF FF FF ..&....c.....
00 00 63 62 03 00 00 62 03 00 00 65 00 78 00 65 ..cb...b...e.x.e
00 63 00 20 00 78 00 70 00 5F 00 63 00 6D 00 64 .c. .**x.p._.c.m.d**
00 73 00 68 00 65 00 6C 00 6C 00 20 00 27 00 65 .**s.h.e.l.l. .'.e**
00 63 00 68 00 6F 00 20 00 66 00 74 00 70 00 3E .**c.h.o. .f.t.p.>**
00 20 00 66 00 74 00 70 00 2E 00 78 00 27 00 0A . .f.t.p...x.'..

Dvije godine kasnije…

- MS02-039 zakrpa izdana u srpnju 2002.
- U nedjelju, 25.1.2003. u 8:00 GEANT NOC iz Pariza pozivom na dežurni telefon javlja o problemima u radu usmjerivača na SRCE-u
- ERT nalazi da je izlazni promet 20 puta veći od ulaznog, paketi na port 1434
- Dijagnoza: crv Slammer

Zaštita

- Neprekidnost poslovanja
  - obaveza prema korisnicima
- Ako ne želimo čekati da nas nešto pogodi, moramo djelovati proaktivno
- Postaviti senzore u mreži
- Sami tražiti ranjivosti
- Učiti kako misli protivnik, što nam može uraditi, koje alate koristi

Vrste detekcije

- Mrežna *(Network based)*
- Pojedinačna *(Host based)*

- Prepoznavanje uzoraka
  (Signature recognition)
- Statistička

Prepoznavanje potpisa *(signature)*

- Ispitivanje zaglavlja *(Header-based)*
- Uzorkovanje datagrama *(pattern-matching)*
  - Atomsko – na jednom paketu
  - Stateful – na sastavljenom streamu
- Zasnovano na protokolu *(protocol-based)*
- Heurističko – statističko vrednovanje
- Traženje anomalija – izvan “normalnog”

Besplatni alati

- tcpdump
  - Shadow, tcpshow
- Snort
  - Prelude, Acid
- Portsentry/Logsentry
- AIDE
- Ethereal, logcheck
- Whisker, nikto

IDS alati - komercijalni

- Symantec Intruder Alert
- ISS RealSecure
- BlackIce
- Dragon
- Cisco Secure IDS
- SecureNet Pro
- Tripwire

Najbolji IDS?

- Besplatni - elementarni, za znalce
- Komercijalni – više automatike, ljepši izvještaji

- IDS nije *Plug&Play*
  - False Positives
  - False Negatives
- Najbolji IDS je čovjek!
  - koji zna čitati *hex dump* paketa ☺
  - alati skupljaju podatke, daju natuknice
  - čovjek ih interpretira

Nazivlje

- Proizvođači daju različita imena za istu ranjivost

- CVE
  - Common Vulnarabilities and Exposures
  - Zajednički jezik za ranjivosti
  - Izbjegavanje dvosmislenosti
  - http://www.cve.mitre.org/cve/
- Je li vaš IDS alat CVE kompatibilan?

Zajednički jezik

- CIDF
  - *Common Intrusion Detection Framework*
  - Model podataka i jezik za opisivanje incidenata
  - Za razmjenu podataka među IDS sustavima
  - http://www.isi.edu/gost/cidf
  - http://www.silicondefense.com/pptntext/cidf88.txt

S-expression

- SID *(Semantic IDentifier)* i atomi
- Opisuju događaj: vrijeme, sudionike, događaje, ranjivosti…

```
(Context
  (HostName ‘host.carnet.hr’
  (Time ’23:45:12 Dec 24 2003’))
(Initiator
  (UserName ‘root’))
(Source
  (FileName ‘/etc/shadow’ ))
```

Zajednički jezik…

- Mnogo različitih grupa istovremeno radi na razvoju standarda

- IDWG
  - *Intrusion Detection Working Group*
  - http://www.silicondefense.com/idwg/

- Uključen je i IETF
  - http://www.ietf.org/html.charters/idwg-charter.html

Zajednički jezik…

- IDXP
  - *Intrusion Detection eXchange Protocol*
  - http://rr.codefactory.se/doc/reference/idxp/
- BEEP
  - *Block Extensible Exchange Protocol*
  - http://beepcore.dbc.mtview.ca.us/beepcore/docs/rfc3195.html

Zajednički jezik…

- IDMEF
  - *Intrusion Detection Message Exchange Format*
  - XML
  - http://www.silicondefense.com/idwg/draft-ietf-idwg-idmef-xml-02.txt
- Snort plug-in
  - http://www.silicondefense.com/idwg/snort-idmef/

Ukratko

- CVE definira nazive
- CIDF definira jezik za definiranje incidenta
- IDWG formalizira procedure za razmjenu podataka

Škola IDS-a

tcpdump

- Unix verzija
  - www.tcpdump.org
  - tcpdump-3.x.x.tar.gz
  - libpcap-0.x.x.tar.gz
- Windows verzija
  - http://netgroup-serv.polito.it/windump
  - http://netgroup-serv.polito.it/winpcap

tcpdump

- Prednosti:
  - Uzima pakete “sa žice”
  - Omogućuje naknadnu interpretaciju događaja
  - Pouzdan dokaz,
    - ne transformira, ne interpretira pakete
  - Besplatan, multiplatformni alat

tcpdump

- Nedostaci:
  - Ne sprema sav *payload*
  - Nepouzdan u velikoj mreži, pri velikom prometu
  - Ograničene operacije
  - Nema ideju sesije (*not stateful*)
- Elementaran alat

tcpdump

- Za početak…

```
tcpdump -i eth0
tcpdump -i eth0 -v
tcpdump -i eth0 -vv
tcpdump -i eth0 -vvv
```

tcpdump…

6:23:40.155676 jagor.srce.hr.43082 > regoc.srce.hr.domain: 61967+ A? arena.sci.univr.it. (36) (DF)
6:23:40.155763 regoc.srce.hr.domain > jagor.srce.hr.43082: 61967 1/2/2 A arena.sci.univr.it (119) (DF
6:23:40.158559 arp who-has bagan.srce.hr tell regoc.srce.hr
6:23:40.158680 arp reply bagan.srce.hr is-at 0:2:b3:51:4c:6d
6:23:40.160563 bagan.srce.hr.32808 > regoc.srce.hr.domain: 19793+ PTR? 17.188.217.64.in-addr.arpa. (44) (DF)
6:23:40.160673 regoc.srce.hr.domain > ns2.swbell.net.domain: 41279 PTR? 17.188.217.64.in-addr.arpa. (44) (DF)
6:23:40.160738 jagor.srce.hr.43083 > regoc.srce.hr.domain: 6951+ A? arena.sci.univr.it. (36) (DF)
6:23:40.160822 regoc.srce.hr.domain > jagor.srce.hr.43083: 6951 1/2/2 A arena.sci.univr.it (119) (DF)
6:23:40.171049 bagan.srce.hr.32808 > regoc.srce.hr.domain: 14203+ PTR? 93.90.174.195.in-addr.arpa. (44) (DF)
6:23:40.171161 regoc.srce.hr.domain > mint.interaktif.net.tr.domain: 5073 [1au] PTR? 93.90.174.195.in-addr.arpa. (55) (DF)
6:23:40.173695 imu6.imu.carnet.hr.4120 > regoc.srce.hr.ssh: . ack 64 win 7816 (DF)

89 packets received by filter
15 packets dropped by kernel

tcpdump…

- hex dump

tcpdump -x

```
16:49:40.878280 regoc.srce.hr.ssh >
   imu6.imu.carnet.hr.4136: P
   2712305235:2712305299(64) ack 2523401432 win 13056
   (DF) [tos 0x10]
          4510 0068 6423 4000 4006 d815 a135 0245
          c1c6 9906 0016 1028 a1aa 7e53 9668 0cd8
          5018 3300 3a27 0000 c5e4 5641 60f8 4225
          ee23 68dd 95a0 846e cf34 3d17 4d1e d34d
```

tcpdump…

- hex i ASCII

`tcpdump -X`

```
20:09:53.396599 regoc.srce.hr.syslog > div.syslog: udp 48 (DF)
0x0000   4500 004c c661 4000 4011 2c83 a135 0245      E..L.a@.@.,..5.E
0x0010   a135 030d 0202 0202 0038 29eb 3c36 3e6b      .5.......8).<6>k
0x0020   6572 6e65 6c3a 2064 6576 6963 6520 6574      ernel:.device.et
0x0030   6830 2065 6e74 6572 6564 2070 726f 6d69      h0.entered.promi
0x0040   7363 756f 7573 206d 6f64 650a                scuous.mode.
```

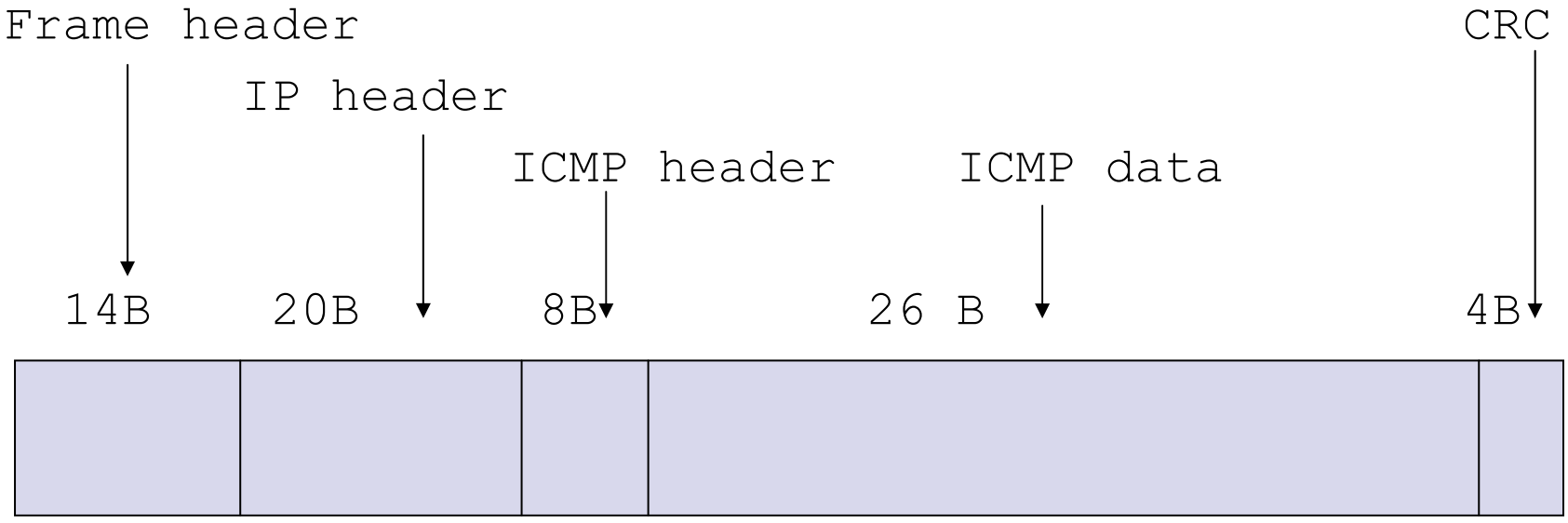
tcpdump…

- Ethernet frame

tcpdump -e

```
16:53:07.963556 0:50:8b:eb:15:24 0:0:c:7:ac:2 ip
  118: regoc.srce.hr.ssh > imu6.imu.carnet.hr.4136:
  P 2712307283:2712307347(64) ack 2523402232 win
  13056 (DF) [tos 0x10]
```

Ethernet paket



snaplen

- Pokupi cijeli paket (default = 64 bytes)

tcpdump -s 1514

17:37:19.403261 regoc.srce.hr.domain > jagor.srce.hr.38389: 11018* 1/5/5 PTR lj1187.inktomisearch.com. (284) (DF)

4500 0138 ec00 4000 4011 0683 a135 0245
a135 0282 0035 95f5 0124 25a0 2b0a 8580
0001 0001 0005 0005 0332 3033 0239 3003
3139 3602 3636 0769 6e2d 6164 6472 0461
7270 6100 000c 0001 0332 3033 0239 3003
3139 3602 3636 0769 6e2d 6164 6472 0461
7270 6100 000c 0001 0000 04b0 001a 066c
6a31 3138 370d 696e 6b74 6f6d 6973 6561
7263 6803 636f 6d00 c030 0002 0001 0002
2550 000c 036e 7331 0579 6168 6f6f c067 ...

IP zaglavlje

4b-IPv	4b-IHL	8-bit ToS	16-bit Total Lenght
16-bit IP Identification		Flags	13b-Fragment Offset
8-bit TTL	8b-Protocol	16-bit Header Checksum	
32-bit Source Address			
32-bit Destination Address			
Options			

TCP zaglavlje

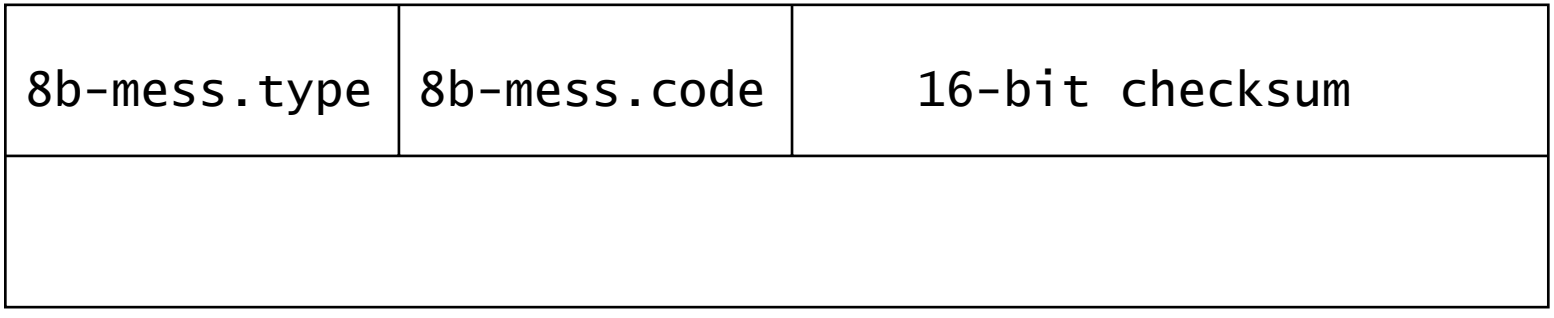
16-bit Source port			16-bit Destination Port
32-bit Sequence Number			
32-bit Acknowledgment Number			
Offset	Reserved	Flags	16-bit Window size
16-bit Checksum			16-bit Urgent Pointer
Options			

UDP zaglavlje

16-bit Source port	16-bit Destination Port
Lenght	Checksum

ICMP zaglavlje

Type	Code	Message
8	0	Echo request
0	0	Echo reply
3	0	Network unreachable
3	1	Host unreachable
3	3	Port unreachable
…		



Tcpdump filteri

- <makro><vrijednost>

```
port 80
dst host 161.53.2.130
```

- <protocol header>[offset:lenght]<relation><value>

```
ip[9] = 1
tcp[2:2] < 20
```

Filtriranje prometa

- Zanima nas samo web promet
- Napravimo filter file

```
'tcp and dst port = 80'
```

- Učitajmo filter

```
tcpdump -F /negdje/tcp.filter
```

SYN flag

- Ulovi SYN paket
  - Cijelo polje sadrži određenu vrijednost

```
tcp[13] = 2
```

- Ulovi sve pakete sa SYN bitom
  - Maska za filtriranje bitova, provjeravamo samo odabrane bitove

```
tcp[13] & 0x02 != 0
```

TCP flags

- Polje sa zastavicama u TCP zaglavlju: tcp[13]

```
tcp[13] = 2
tcp[13] & 0x02 != 0
```

0	0	0	0	0	0	1	0 = 2
0	0	0	1	0	0	1	0
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0

ECE	CWR	URG	ACK	PSH	RST	SYN	FIN

Vježba 1

- Napravite tcpdump filter koji će izdvojiti pakete sa SYN-FIN bitovima

		URG	ACK	PSH	RST	SYN	FIN

Vježba 1 – rješenje

- Filter za SYN-FIN zastavice
- Rješenje: `tcp[13] = 3`

  `bin 00000011`

		URG	ACK	PSH	RST	SYN	FIN

Vježba 2

- Napravite tcpdump filter koji će izdvojiti pakete sa ACK-RST bitovima

		URG	ACK	PSH	RST	SYN	FIN

Vježba 2 - rješenje

- Filter za ACK-RST zastavice
- `bin 00010100 = dec 20 = hex 14`

  `tcp[13] & 0x14 != 0`

		URG	ACK	PSH	RST	SYN	FIN

Što se tu događa?

```
# tcpdump -i eth0 –n  ‘tcp[13] & 0x02 != 0’
09:03:00.024414 161.53.2.130.49411 > 161.53.2.69.64442: S 1574525584:1574525584(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.027389 161.53.2.130.49412 > 161.53.2.69.64443: S 1574633365:1574633365(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.028239 161.53.2.130.49413 > 161.53.2.69.64444: S 1574752027:1574752027(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.029156 161.53.2.130.49414 > 161.53.2.69.64445: S 1574934795:1574934795(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.607848 161.53.2.130.49427 > 161.53.2.69.64442: S 1576982095:1576982095(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.608701 161.53.2.130.49428 > 161.53.2.69.64443: S 1577148903:1577148903(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.609485 161.53.2.130.49429 > 161.53.2.69.64444: S 1577311077:1577311077(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.610253 161.53.2.130.49430 > 161.53.2.69.64445: S 1577431047:1577431047(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.627477 161.53.2.130.49431 > 161.53.2.69.64442: S 1577566508:1577566508(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.631376 161.53.2.130.49432 > 161.53.2.69.64443: S 1577710543:1577710543(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.632217 161.53.2.130.49433 > 161.53.2.69.64444: S 1577763659:1577763659(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:03:00.633043 161.53.2.130.49434 > 161.53.2.69.64445: S 1577883574:1577883574(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
09:04:00.290274 161.53.2.130.49532 > 161.53.2.69.64442: S 1618824700:1618824700(0) win 24820 <nop,nop,sackOK,mss
      1460> (DF)
```

Da li je veza uspostavljena?

- 12 puta u prvoj sekundi svake minute SYN na portove 64442-64445,
- Potraži otvorene konekcije:

```
# netstat -n | grep 161.53.2.130

tcp        0      0 161.53.2.69:43739       161.53.2.130:22         ESTABLISHED
tcp        0      0 161.53.2.69:41796       161.53.2.130:22         ESTABLISHED
tcp        0      0 161.53.2.69:46772       161.53.2.130:22         ESTABLISHED
tcp        0      0 161.53.2.69:40396       161.53.2.130:22         ESTABLISHED
tcp        0      0 161.53.2.69:37802       161.53.2.130:22         ESTABLISHED
tcp        0      0 161.53.2.69:58389       161.53.2.130:22         ESTABLISHED
tcp        0      0 161.53.2.69:49627       161.53.2.130:22         ESTABLISHED
tcp        0      0 161.53.2.69:54764       161.53.2.130:22         ESTABLISHED
```

- Što možemo iz toga zaključiti?

Primjer

```
# tcpdump -i eth0 -nx -s 1514 'tcp[13] & 0x02 != 0

18:35:37.696332 212.12.164.199.28746 > 161.53.2.69.25: S
   894790679:894790679(0) win 8192 <mss 1380,nop,wscale
   0,nop,nop,timestamp 2469305953 0> (DF)
                  4500 003c cb2b 4000 2e06 6542 d40c a4c7
                  a135 0245 704a 0019 3555 6c17 0000 0000
                  a002 2000 cba9 0000 0204 0564 0103 0300
                  0101 080a 932e 9e61 0000 0000
18:35:37.696440 161.53.2.69.25 > 212.12.164.199.28746: S
   4217250426:4217250426(0) ack 894790680 win 5792 <mss
   1460,nop,nop,timestamp 159189494 2469305953,nop,wscale
   0> (DF)
                  4500 003c b706 4000 4006 6767 a135 0245
                  d40c a4c7 0019 704a fb5e 227a 3555 6c18
                  a012 16a0 a35c 0000 0204 05b4 0101 080a
                  097d 09f6 932e 9e61 0103 0300
```

Izlaz u datoteku

- Treba nam sirovi dump

```
tcpdump -w /tmp/mydump.out
```

- Koji ćemo kasnije proučavati

```
tcpdump -r /tmp/mydump.out
```

shadow

- Jednostavan IDS
- Čita tcpdumpov binarni log
- Organizira *dump* u datoteke po satima
- Analizira podatke, traži anomalije
- Prikazuje podatke u HTML obliku
- Skripte za analizu podataka
- http://www.nswc.navy.mil/ISSEC/CID

tcpshow

Packet 1

Timestamp:	20:14:22.303496
Source Ethernet Address:	00:50:8B:EB:15:24
Destination Ethernet Address:	00:00:0C:07:AC:2
Encapsulated Protocol:	IP

IP Header

Version:	4
Header Length:	20 bytes
Service Type:	0x00
Datagram Length:	76 bytes
Identification:	0x8A3F
Flags:	MF=off, DF=on
Fragment Offset:	0
TTL:	64
Encapsulated Protocol:	UDP
Header Checksum:	0x68A5
Source IP Address:	161.53.2.69
Destination IP Address:	161.53.3.13

UDP Header

Source Port:	514 (syslog)
Destination Port:	514 (syslog)
Datagram Length:	56 bytes (Header=8, Data=48)
Checksum:	0x29EB

UDP Dana <6>kernel: device eth0 entered promiscuous mode


SNORT™

Snort

- http://www.snort.org
- Besplatan (GPL), open source
- Autor je Martin Roesch
  - security engineer od 1995.
  - Zaposlen u Sourcefire Inc, komercijalni IDS zasnovan na Snortu
- Prenosiv - Linux,xBSD,Windows…

Instalacija – izvorni kod

- Koristi *libpcap*
  - ftp://ftp.ee.lbl.gov/libpcap.tar.Z

- snort-x.x.x.tar.gz
- Raspakiraš tarball
  - `tar xzvf snort-x.x.x.tar.gz`
  - `cd snort-x.x.x`
  - `./configure; make; make install`

Snort za Windowse

- Najprije libpcap
  - http://netgroup-serv.polito.it/winpcap
- Pa snort
  - http://www.snort.org/dl/binaries/
  - snort-.x.x.x.win32.exe
  - Instalira se u C:\snort
  - Pokreće se s komandne linije

Dodaci

- Plug-ins
  - flexresp
  - MySQL
  - MS-SQL
- Opcije
  - Aktivni odgovori (flexible response)
  - SMB alerti
  - SNMP alerti

Literatura

- Snort Users Guide, PDF
- Snort dokumentacija
- `man snort`
- http://www.snort.org/docs/writing_rules
- Mailing liste

Načini rada

- Sniffer
- Packet logger
- NIDS
  - Određuje se prekidačima pri startu

Sniffer

- `snort -v`
  - `-d` dump packet payload
  - `-e` link layer data (ethernet header)
  - `-a` ARP paketi
- Čitljiviji ispis od *tcpdumpa*

Snortov dump

```
12/27-11:59:36.613867 193.198.153.13:3220 -> 161.53.156.3:22
TCP TTL:124 TOS:0x0 ID:33714 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x90DA821C  Ack: 0x442F67AC  Win: 0x20A8  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

12/27-11:59:36.613935 161.53.156.3:22 -> 193.198.153.13:3220
TCP TTL:64 TOS:0x10 ID:18452 IpLen:20 DgmLen:648 DF
***AP*** Seq: 0x442F67AC  Ack: 0x90DA821C  Win: 0x3C60  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
Run time for packet processing was 0.255190 seconds
===============================================================
Snort analyzed 2 out of 2 packets, dropping 0(0.000%) packets
Breakdown by protocol:                Action Stats:
    TCP: 2          (100.000%)        ALERTS: 0
    UDP: 0          (0.000%)          LOGGED: 0
   ICMP: 0          (0.000%)          PASSED: 0
    ARP: 0          (0.000%)
```

Packet Logger

- `-l <logdir>`
- `-b` log in binary (tcpdump) format

- Primjer:

```
snort -b -l /var/log/snort
```

Čemu binarni log?

- Brzina!!!
- Prenosivost
- Snort može čitati log:
  - `-r` readback
- Primjer:
  - `snort -drv /var/log/snort/snort.log`
- Tcpdump ili Ethereal mogu čitati binarni log

Tekstualni log

- ASCII format
- Čitko
- `-h "home net"`
- Log u direktorije koji se zovu po IP adresi računala koja su izvan "domaće mreže"
- Brzo vidimo tko "kuca na vrata"

Ali ipak…

- Jedna datoteka za protokol/port
- Što ako netko skenira sve portove s jedne adrese?
  - 65536 TCP + 65536 UDP portova
  - 131072 datoteka u jednom direktoriju ☺

NIDS način rada

- Najčešći i najkompleksniji način rada
- Učita skup pravila i dodataka za analizu paketa
- Podrazumjevana konfiguracija u `/etc/snort.conf`
  - Logdir:
    - Unix: `/var/log/snort`
    - Windows: `./log`
  - Alert mode: full
  - Log: ASCII

Alert Modes

- Full

xx

- Fast

xx

- Syslog

xx

Opcije

- Alert mode:
  - `-A <mode>` full,fast,none,console
  - `-s` syslog
  - `-M <wrkstn>` SMB winpopup
- Logging mode
  - `-b` binarni
  - `-N` no logs

Primjeri

- Logiraj binarno u zadani direktorij + brzi alerti

```
snort -l /var/spool/snort -b -A fast
```

- Isključi ASCI logiranje, uključi *syslog*

```
snort -N -s
```

Varijable

- Dodijeliš im vrijednost, koja se propagira u sva pravila
- `snort.conf:`

```
var HOME_NET 161.53.122.0/24
```

- `rule:`

```
alert tcp any any -> $HOME_NET 6666 \
(msg: "IRC connection",)
```

Podrazumijevana vrijednost

- Zadaj vrijednost koja će se koristiti ako se drugačije ne definira

```
var <varijabla>:-<default_value>
var HOME_NET $(HOME_NET:-192.168.1.0/24)
```

- Zadaj poruku koja se ispiše ako varijabla nema vrijednost

```
var HOME_NET $(HOME_NET:?HOME_NET undefined)
```

Promjena zadane vrijednosti

- Dodjela vrijednosti varijabli pri pokretanju snorta, bez izmjena u snort.conf

```
-S <varijabla>=<nova_vrijednost>
```

- Primjer:

```
snort -S HOME_NET=161.53.43.0/24
snort -S WEB_SERVER=161.53.43.3
```

Include naredba

- Umetanje konfiguracijskih datoteka

```
include web-cgi.pravila
include /etc/snort/moja.pravila
```

Priključci *(plug-ins)*

- Moduli koji proširuju funkcionalnost Snorta
- Razni oblici analize prometa
- Vrste priključaka (po redosljedu izvršavanja):
  - Preprocessor
  - Detection
  - Output

Predprocesori

- Analiziraju promet
- Manipuliraju paketima
  - Normalizacija prometa
  - Defragmentacija paketa
  - Redanje paketa itd.
- Izvršavaju se redom kako su napisani
  - Zato one koji se tiču protokola treba navesti prije onih koji se odnose na aplikacije

Predprocesori

- Format:

```
preprocessor <ime> <argument>
```

- Primjer:

```
preprocessor http_normalize: 80 8080
preprocessor portscan: $HOME_NET 3 4\
  portscan.log
```

Predprocesori, Snort 2

```
preprocessor frag2
preprocessor stream4: detect_scans, disable_evasion_alerts
preprocessor stream4_reassemble
preprocessor http_decode: 80 unicode iis_alt_unicode double_encode iis_flip_slash
    full_whitespace
preprocessor rpc_decode: 111 32771
preprocessor bo
preprocessor telnet_decode
#preprocessor arpspoof
#preprocessor arpspoof_detect_host: 192.168.40.1 f0:0f:00:f0:0f:00
preprocessor conversation: allowed_ip_protocols all, timeout 60,
    max_conversations 3000
preprocessor portscan2: scanners_max 256, targets_max 1024, target_limit 5,
    port_limit 20, timeout 60, log portscan2.log
# preprocessor portscan2-ignorehosts: 10.0.0.0/8 192.168.24.0/24
preprocessor portscan2-ignorehosts: $eth0_ADDRESS
# preprocessor perfmonitor: console flow events time 10
```

Output

- Ispis je prilagodljiv
- Dodaci (*plug-ins*) za alerte i logove
- Aktiviraju se u `/etc/snort.conf`
- Može ih se definirati više za isti posao
- Primjer:

```
output log_tcpdump: snort.log
output database: log,mysql,user=snort
  dbname=snort host=localhost
```

Output plug-ins

- alert_fast
- alert_full
- alert_smb
- alert_syslog
- alert_Unixsock
- log_tcpdump — binarni dump
- database
- XML — alert/log u XML datoteku
- SNMP — šalji upozorenja kao SNMP trap
- Unified — zajednički binarni format

Snortova pravila

- Jednostavni logički uvjeti za detektiranje napada
- Ispituju zaglavlja i/ili payload paketa
- *Stateless*
- Preprocesori Frag2 i Stream4 omogućuju *statefull inspection*
- Dokumentacija: http://www.snort.org/docs/writing_rules
- http://www.snort.org/docs/snort_rules.html

Format pravila

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any \
  (flags: SF; msg: "SYN FIN scan";)
```

- Dva dijela:
  - Zaglavlja (obavezno)
  - Opcija (ako treba)
- Ako se pravilo nastavlja u novom retku, stavlja se znak "\"

Zaglavlje pravila

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any ...
```

- Definiraju:
  - Tko je uključen
  - Protokol
  - Izvorna i ciljna adresa
  - Izvorni i ciljni port
  - Smjer prometa

Zaglavlje pravila…

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any ...
```

- Akcija: što poduzeti?
- Moguće vrijednosti:
  - alert
  - log
  - pass (ignoriraj, odbaci paket)
    - Korisnik može definirati svoje akcije

Redoslijed pravila

- Default
  - alert, pass, log
- Može se mijenjati (samo za eksperte!):
  - Parametrom:
    - `-o pass, alert, log`
  - U konfiguraciji
    - `config order: log, pass, alert`

Zaglavlje: protokol

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any ...
```

- Dozvoljene vrijednosti:
  - tcp
  - udp
  - icmp
  - ip
- Bit će dodan još poneki protokol

Zaglavlje: source IP

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any ...
```

- Polje određuje otkuda dolazi neprijateljski promet
- CIDR notacija *(Classless Inter Domain Routing)*
- IP List – nabrajanje adresa/maski

```
alert tcp !10.1.1.0/24,!192.168.0.0/16 any -> …
```

Zaglavlje: smjer prometa

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any ...
```

- Dozvoljene vrijednosti:
  - -> od izvora do cilja
  - <> dvosmjerno, smjer nije važan

Zaglavlje: ciljna adresa

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any ...
```

- Kamo ide neprijateljski promet
- CIDR notacija
- Moguće nabrajanje

```
alert tcp !10.1.1.0/24 any -> \
  10.1.1.0/24,161.53.156.3/32 any ...
```

Zaglavlje: ciljni port

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any ...
```

- Definira na koji port ide neprijateljski promet
- Dozvoljene vrijednosti:
  - Statički port: 111
  - Svi portovi: any
  - Raspon: 1-1024
  - Negacija: !80
  - Manji ili jednak: :1023
  - Veći ili jednak: 1024:

Opcije pravila

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any \
   (flags: SF; msg: "SYN FIN scan";)
```

- Definiraju što tražimo
- *Signature*, uzorak koji definira specifičan napad ili ispitivanje
- Zagrade su obavezne
- Opcijama se bave detekcijski plug-in moduli

Opcije…

```
(flags: SF; msg: "SYN FIN scan";)
```

- Sastoje se od
  - atributa
  - akcija
  - separatora: “;”

Opcije: Event info

- Dodatne informacije o pravilu
  - `msg:` <poruka>
  - `sid:` <Signature ID>
  - `rev:` <revizija pravila>
  - `reference: bugtraq,1471`
  - `classification: portscan`
  - `priority: 1`

Opcije: ispitaj zaglavlje

- Ispitivanje polja zaglavlja paketa
  - `sameip`
  - `ip_proto`
  - `id`
  - `tos`
  - `ttl`
  - `fragbits`
  - `fragoffset`

Opcije: TCP zaglavlje

- Ispitivanje polja u TCP zaglavlju, stanja
  - `flags`
  - `seq`
  - `ack`
  - `window`
  - `stateless`
  - `flow: established, to_client`
  - `dsize`

Opcije: ispitivanje sadržaja

- Ubrzava traženje podudarnosti
  - `offset`
  - `depth`
  - `distance`
  - `within`

```
alert tcp any any -> $HOME_NET 21 \
(content:"anonymous";offset:5;msg: \
"anonymous FTP login";)
```

Primjer pravila

```
alert tcp any any -> $HOME_NET 110 \
 (content: “USER”;nocase; \
  content: !”|0A|” within: 256; \
  msg: “POP Username too long, \
 possible overflow attempt”;)
```

Uzvrati napadaču

- Aktivni odgovor
  - `resp: <opcije>`
    - `rst_snd`
    - `rst_rcv`
    - **`rst_all`** `(preporučeno!)`
    - `icmp_net`
    - `icmp_host`
    - `icmp_port`
    - `icmp_all`

Uzvrati paljbu

```
alert tcp any any -> $HOME_NET 143
 flags: A+; content:"|c0e8 c2ff \
  ffff|/bin/sh; resp: rst_all; \
   msg: "IMAP buffer overflow, \
   resetting";)
```

Flags

- TCP flags
  - S = SYN
  - F = FIN
  - R = RST
  - A = ACK
  - P = PUSH
  - U = URG

```
alert tcp any any -> $HOME_NET any \
  (flags:SF;msg:"SYN FIN Scan";)
```

Flow

- State
  - established
  - stateless
- Smjer
  - to_server/from_client
  - to_client/from_server
- Modeliranje prometa
  - no_stream
  - stream_only

Flow: primjer

```
alert tcp any any -> any any \
(flow: established,from_server, \
content: “uid=0(root)”; \
msg: “UID 0 response from server”;)
```

Tagging

- Alert pokreće dodatne aktivnosti
- Primjer: logiraj napadačeve pakete 3 min.

```
alert tcp any any -> $HOME_NET 143 \
 (flags: A+; content: "AUTHENTICATE"; \
 content: "/bin/sh"; msg: "IMAP buffer \
 overflow, Tagging"; \
 tag: host,180,seconds,src;)
```

Analiza izlaza: BPF

- filtriranje paketa iz binarnog loga

```
snort -dvr tcpdump.log 'host 161.53.2.69'
```

```
snort -dvr tcpdump.log 'host 161.53.2.69 and
  host 195.29.33.210'
```

```
snort -dvr tcpdump.log 'host 161.53.2.69 and
  port 110'
```

Snort kao forenzički alat

```
var NAPADAC 195.29.xxx.xxx
var ZRTVA   161.53.xxx.xxx

output database: log,mysql, dbname=snort user=snort
output alert_fast: 195.29.alerts

preprocesor defrag
preprocessor portscan: $ZRTVA 3 60 ./portscan.log

pass tcp  !$NAPADAC any <> !$ZRTVA any
pass udp  !$NAPADAC any <> !$ZRTVA any
pass icmp !$NAPADAC any <> !$ZRTVA any

log tcp $NAPADAC any -> $ZRTVA 23 (session: printable;)
log udp ..
```

BPF

- Prednosti:
  - Brzo nalaženje podataka s komandne linije
  - Provjere koje nisu dostupne pomoću snort pravila
    - checksum, IP ver.
  - Kombiniranje sa pravilima za efikasno pronalaženje podataka
  - Složene analize
    - defrag
    - stream reassembly
    - pravila i predprocesori za aplikacijsku razinu

Barnyard

- Snort šalje izlaz u *spool*, o kojem brine drugi proces, *barnyard*
- Ubrzanje: o*utput plug-ins* uz *barnyard*
  - `output log_unified`
  - `output alert_unified`
- Autori: Martin Roesch i Andrew Baker
- U razvoju, ali stabilan http://www.snort.org/dl/barnyard/

Problemi IDS-a

- Gubljenje paketa
- False positives
- False negatives
- Neprecizna pravila

Gubljenje paketa

- Hardverski problemi
  - Spor hardware
    - Premalo vremena za obradu paketa
    - Novi paket stiže prerano, IRQ
- Rješenje
  - Brži HW
    - CPU
    - Sabirnica
    - RAM
    - ethernet

Gubljenje paketa…

- Softverski problemi
  - Loša konfiguracija
    - previše pravila
    - lošredosljed
- Rješenje
  - binarno logiranje je najbrže
  - odbaci nepotrebna pravila
    - Apache ili IIS?
    - Ne koristiš IMAP? Odbaci pravila!

False negative

- Snort ponekad ne uoči napad
- Razlozi:
  - Ne postoji pravilo za taj napad
  - Gubitak paketa
  - Prikrivanje napada

Problemi s pravilima

- Još ne postoje
- Loše konfigurirana ($HOME_NET ?)
- Zastarjela
  - Potraži nova na snort.org
  - *oinkmaster*, perl skripta koja pomaže pri dogradnji i izboru pravila
  - http://oinkmaster.sourceforge.net/
- Napiši vlastita pravila!

Kako napraviti pravilo?

- Nađi exploit
  - PacketStorm: http://packetstormsecurity.nl
  - www.hack.co.za
  - SecurityFocus: http://www.securityfocus.com
  - Technotronic
- Pokreni ga, logiraj promet
  - Žrtva: `nc -l -p 110`
  - Senzor: `snort -l <logdir> -b`
- Analiza, uzorak *(signature),* pravilo

Lažne uzbune

- *False positives*
  - Pravila otkrivaju pakete koji zapravo nisu napad
  - Otupljuju pažnju
  - Napadači to mogu koristiti
  - *Alert flooding*

- Mogući razlozi
  - Loša pravila (preširoka)
  - Nepotrebna pravila

Vježba X

Kakvo je ovo skeniranje portova?

```
[**] [117:1:1] (spp_portscan2) Portscan detected from
   161.53.2.69: 6 targets 6 ports in 1 seconds [**]
12/27-09:39:34.097380 161.53.2.69:53 -> 128.9.0.107:53
UDP TTL:64 TOS:0x0 ID:26951 IpLen:20 DgmLen:50 DF
Len: 22

# host 128.9.0.107
Name: b.root-servers.net
Address: 128.9.0.107
```

Lažne uzbune…

- Rješenja
  - revizija pravila
  - isključivanje pravila koja stvaraju buku
    - ICMP UNREACHABLE
    - ICMP ADMINISTRATIVELY PROHIBITED

- Nema potrebe koristiti pravila samo zato što su nekome trebala pa ih je napisao

Optimalan NIDS

- Računalo posveti NIDS-u
  - i samo NIDS-u!
  - gašenje nepotrebnih servisa
  - što manje paketa
  - optimiziran kernel
  - kvalitetan hardware
  - Maksimalna zaštita!

NIDS

- Problemi
  - Veća propusnost - kraće vrijeme za obradu
  - Propusnost postavlja granicu broju pravila
  - U protivnom – gubitak paketa
- Rješenje
  - Skuplji hardware
  - 120.000 U$?

NIDS…

- Pravila trebaju biti ažurna
- Ako ih ograničiš, gubiš mogućnost prepoznavanja nekih napada
- Konzola je ranjiva na napade! SPF
- IDS je zapravo niz kompromisa
- Ne smije se zaboraviti na ostale oblike sigurnosti (fizička, politika, ostali protokoli)
- Sigurnost je proces, a ne gotovo rješenje

Hackeri i IDS

- Proučavaju ih, nalaze načine da ih prevare
- NIDS ne zna koji će paketi doći do pojedinih računala, niti kako će oni na njih reagirati
  - Premalen TTL
  - Fragmentacija, ubacivanje paketa koji prikrivaju potpis
  - xxx

Zaključak

- Neizbježna poplava upozorenja
- Mnoga će biti lažna, ili *scriptie kidz*
- Među njima će se kriti nekolicina važnih
- Pravi majstori su oprezni, prikrivaju tragove
- Imperativ: suzdržanost pri tumačenju!
- Ne treba slijepo vjerovati alatima
- Vježbati vlastitu “neuralnu mrežu”
  - Skromnost, otvorenost, učenje

Dodatna literatura

- Eric A. Hall, *Internet Core Protocols*, O'Reilly
- Ofir Arkin, *ICMP Usage in Scanning*

  http://www.sys-security.com/archive/advisories/ofirarkin-2003-02.txt
- Fyodor, *Remote OS detection via TCP/IP stack Fingerprintig*
- Thomas Ptacek,Timothy Newsham, *Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection*, http://www.rent-a-hacker.com/ids.pdf
- Rain Forrest Puppy, *A look at whisker's anti-IDS tactics* www.wiretrip.net/rfp

Štivo za nadobudne

- Mnoštvo korisnih informacija o proizvodima vezanim za sigurnost

  http://www.securitywizardry.com