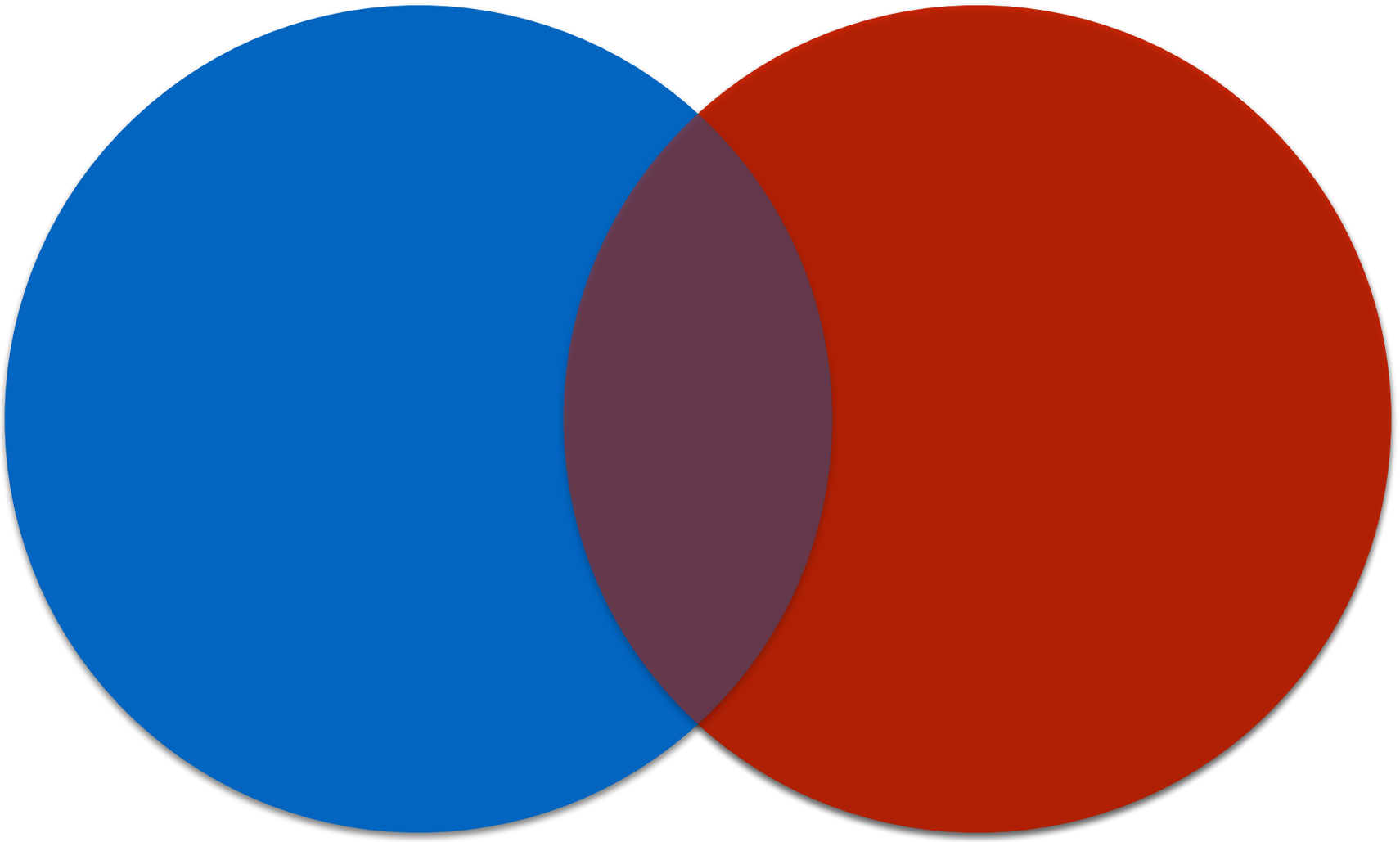
Threat Hunting with

<profile>
<name>**Xavier Mertens**</name>
<nick>**xme**</nick>
<jobs>
<day>**Cyber Security Freelance**</day>
<night>**Blogger, ISC Handler, Hacker**</night>
</jobs>
<![CDATA[
https://xavier.mertens.consulting
https://blog.rootshell.be
https://isc.sans.edu
https://www.brucon.org
]]>
</profile>

Me ❤ OSSEC

- Daily usage of OSSEC to monitor my own infrastructure
- OSSEC Advocate
- Performed customer's projects based on OSSEC
- My current instance has 5y of backlog (1.4B events :-)
- First mention in a blog post: 2010
- Contributions to the project:
  - CEF support
  - GeoIP support

Blue + Red = Purple



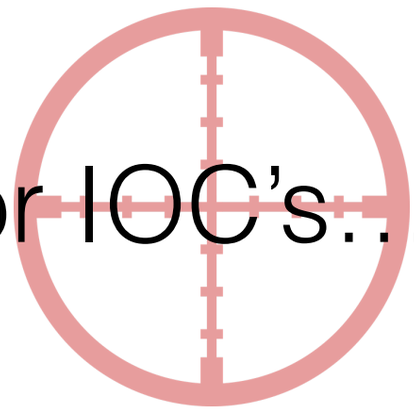
Threat Hunting 101

"The process of **proactively** and iteratively searching through networks to **detect** and isolate advanced threats that **evade** existing security solutions."

Thank you Wikipedia :)

Threat Hunting 101

It does not resume to searching for IOC’s…



… but it’s a good first step!

Threat Hunting 101

It is based on tools

… but also processes!

Threat Hunting 101

Use cases are key!

Read:
Focus on what is important to detect for
you!

IOC’s

- IP addresses
- Domain names, FQDN
- Hashes (MD5, SHA1, SHA256)
- Users
- User-Agent
- Email addresses
- Processes
- Files
- Mutexes
- …

IOC's

<Any data valuable in your $ENV>

The value of an IOC is based on its context!
(Quantity <> Quality)

Who knows OSSEC?

OSSEC 101

Watching

OSSEC watches it all, actively monitoring all aspects of system activity with file integrity monitoring, log monitoring, rootcheck, and process monitoring. With OSSEC you won't be in the dark about what is happening to your valuable computer system assets.

Alerting

When attacks happen OSSEC lets you know through alert logs and email alerts sent to you and your IT staff so you can take quick actions. OSSEC also exports alerts to any SIEM system via syslog so you can get real-time analytics and insights into your system security events.

Everywhere

Got a variety of operating systems to support and protect? OSSEC has you covered with comprehensive host based intrusion detection across multiple platforms including Linux,Solaris, AIX, HP-UX, BSD, Windows, Mac and VMware ESX.

OSSEC 101

- ☑ Client - Server based (agents)
- ☑ UNIX | Windows | MacOS
- ☑ Log collection & analysis
- ☑ Syscheck (FIM)
- ☑ Rootcheck
- ☑ Interaction with 3rd party tools
- ☑ Active-Response
- ☑ Console tools only(*)
- ☑ Server running on UNIX only
- ☑ Docker available

(*) Alternative web frontends available like Wazuh (https://wazuh.com/)

OSSEC 101

```
$ tree /var/ossec -L 1
/var/ossec
|-- active-response
|-- agentless
|-- bin
|-- etc
|-- lists
|-- logs
|-- queue
|-- rules
|-- stats
|-- tmp
`-- var
```

Your Mission…

Let’s see how we can configure OSSEC with the help of third party tools / data to detect suspicious activities on a host

Your Mission…

- ☑ Suspicious DNS activity
- ☑ Suspicious files
- ☑ Suspicious processes

Expected time per lab: 20 minutes

Online Lab

Requirements:
Internet connectivity and a SSH client
Some UNIX command line Fu!

- Each students has his/her Amazon EC2 host
- Select an IP address on: https://pad.xameco.net/p/ossecpts19
- Connect to your instance
- Do **NOT** misuse or connect to other hosts!

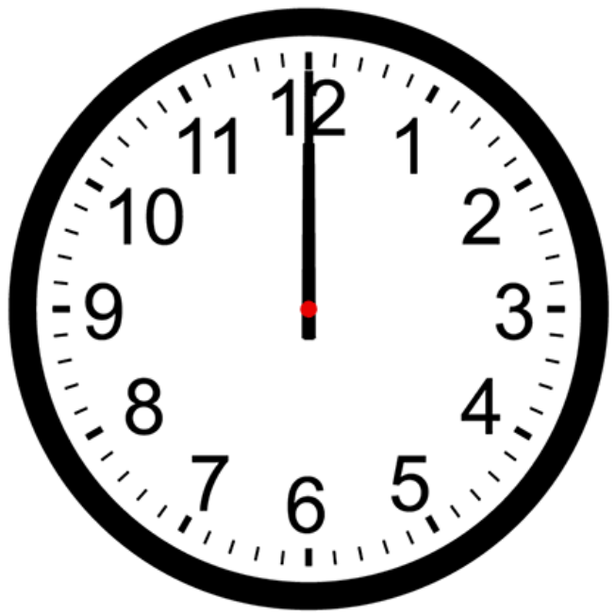
Online Lab

```
ssh -p 443 student@<your-IP-address>
Password: OSSECpts19
```

```
Root access: sudo -s
```

(Feel free to use your beloved editor/shell)

Up to You!



Lab #1

Detecting infected hosts trying to contact their C2 server

Monitoring of DNS traffic is a gold mine to spot infected computers!

Lab #1

OSSEC can use ‘lists’ to query any fields from rules

```
<rule id="99002" level="10">
    <decoded_as>bind9</decoded_as>
    <list field="url">lists/baddomains</list>
    <description>
        DNS query for malicious domain!
    </description>
  </rule>
```

Lab #3

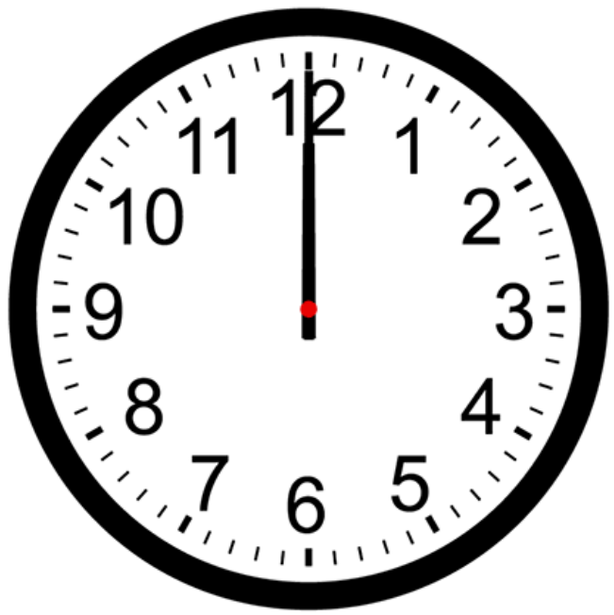
Which domains to search for?

`http://mirror1.malwaredomains.com/files/justdomains`

Lab #1

```
# cd /home/student/lab1
# more README.txt
```

Up to You!



Lab #2

Detecting suspicious files

Suspicious or unknown files on a file system might indicate that a system has been compromized!

Lab #2

OSSEC has a feature called ‘rootcheck’ to detect potential rootkits.

Lab #2

Let’s grab a list of bad files from a MISP instance and feed OSSEC!

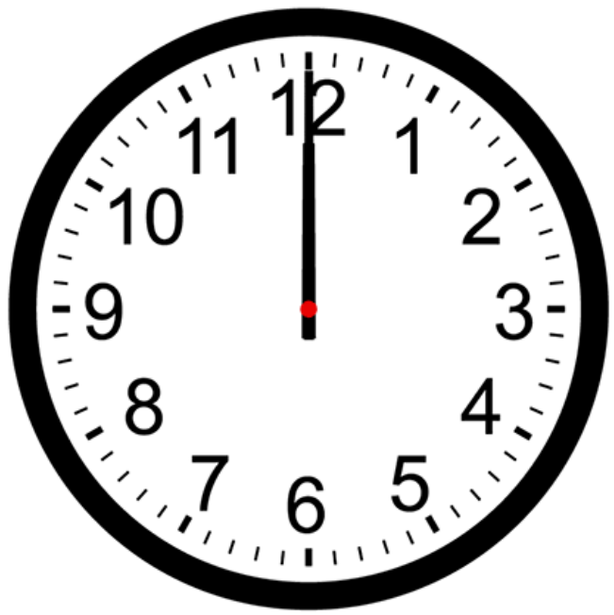
```
# ./mof.py -t 15d -o /var/ossec/etc/shared/myfiles.txt
```

Source: https://raw.githubusercontent.com/xme/toolbox/master/mof.py

Lab #2

```
# cd /home/student/lab2
# more README.txt
```

Up to You!



Lab #3

Detecting running suspicious processes

Unknown processes running on a host are usually bad signals.
It may indicate a compromised host by a trojan, a RAT or a cryptominer…

Lab #3

OSSEC has a feature to monitor output from scripts:

```
<localfile>
    <log_format>command</log_format>
    <command>df -P</command>
</localfile>
```

Lab #3

Let’s grab a list of running processes and compare them with a list of “bad” ones

```
<localfile>
    <log_format>full_command</log_format>
    <command>find /proc -name comm -exec cat "{}" \; \
            2>/dev/null |sort -u</command>
    <frequency>180</frequency>
</localfile>
```

Lab #3

What to search for?

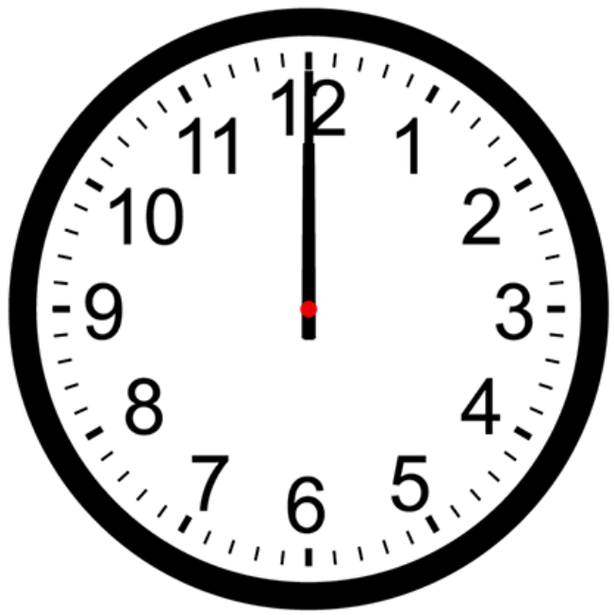
```
AnXqV.yam BI5zj Carbon Duck.sh Guard.sh JnKihGjn
KGlJwfWDbCPnvwEJupeivI1FXsSptuyh NXLAi XJnRj accounts-daemon acpid askdljlqw
atd bonn.sh bonns carbon conn.sh conns crypto-pool ddg donns gekoCrw
gekoCrw32 ir29xc1 irpbalanc1 jIuc2ggfCAvYmluL2Jhc2gi jaav jva kw.sh
kworker34 kxjd lexarbalanc1 lower.sh lowerv2.sh lowerv3.sh minerd minergate
minergate-cli minexmr mixnerdx mule mutex myatd performedl polkitd pro.sh
pubg pvv root.sh rootv2.sh rootv3.sh servcesa sourplum stratum vsp watch-
smart ysaydh AnXqV.yam BI5zj Carbon Duck.sh Guard.sh JnKihGjn
KGlJwfWDbCPnvwEJupeivI1FXsSptuyh NXLAi XJnRj accounts-daemon acpid askdljlqw
atd bb bonn.sh bonns carbon conn.sh conns crypto-pool ddg donns gekoCrw
gekoCrw32 gekoba2anc1 gekoba5xnc1 gekobalanc1 gekobalance gekobalanq1
gekobnc1 ir29xc1 irpbalanc1 irqba2anc1 irqba5xnc1 irqbalance irqbnc1
jIuc2ggfCAvYmluL2Jhc2gi jaav jva kw.sh kworker34 kxjd lexarbalanc1 lower.sh
lowerv2.sh lowerv3.sh minerd minergate minergate-cli minexmr mixnerdx mule
mutex myatd performedl polkitd pro.sh pubg pvv servcesa sourplum stratum
tratum vsp watch-smart wget yam ysaydh
```

Source: https://isc.sans.edu/forums/diary/Crypto+Mining+Is+More+Popular+Than+Ever/24050/

Lab #3

```
# cd /home/student/lab3
# more README.txt
```

Up to You!



Wrap-Up

- ☑ Open source tools to the rescue!
- ☑ Use free data sources for IOCs
- ☑ Know your infrastructure!
- ☑ Be proactive!

About Alerts

- ☑ Local log files
- ☑ JSON (ELK, Splunk, …)
- ☑ Email notifications
- ☑ Syslog (CEF)

```
10:55:17.578190 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), \
   length 77: 127.0.0.1.38048 > 127.0.0.1.7777: Flags [P.], seq 1:12, ack 1, \
   win 342, options [nop,nop,TS val 1437796971 ecr 1437795587], length 11
        0x0000:  4500 003f 189c 4000 4006 241b 7f00 0001  E..?..@.@.$.....
        0x0010:  7f00 0001 94a0 1e61 97cd 1d9a b8d8 37b8  .......a......7.
        0x0020:  8018 0156 fe33 0000 0101 080a 55b3 0a6b  ...V.3......U..k
        0x0030:  55b3 0503 5468 616e 6b20 596f 7521 0a    U...Thank.You!.
```

@xme | xavier@rootshell.be