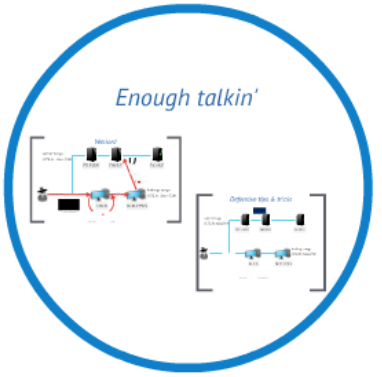
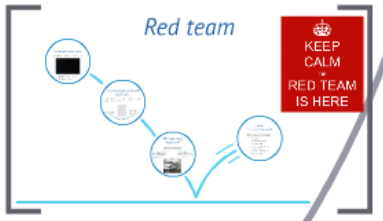
Time to evolve?

Applying red and blue team CTF tactics in IT security.

Online Prezi:

http://prezi.com/a6vwtshrqjzg/



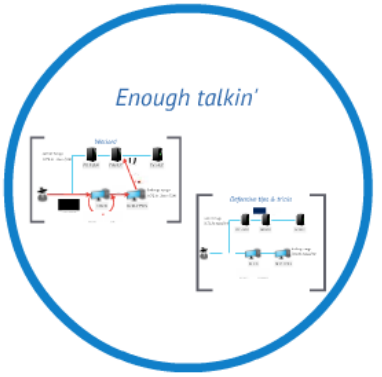


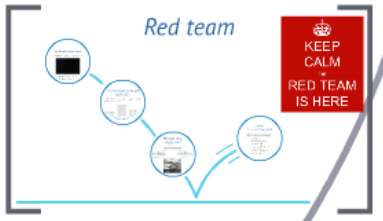
Time to evolve?

Applying red and blue team CTF tactics in IT security.

Online Prezi:

http://prezi.com/a6vwtshrqjzg/

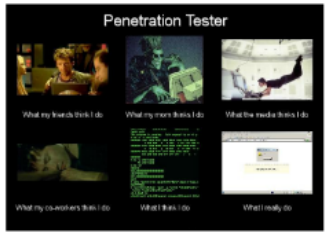




Intro

David Szili

dimension data



Mihaly Zagon

Prezi

The Idea

Cyberlympics 2012

CTF tactics in real life?

The Problem

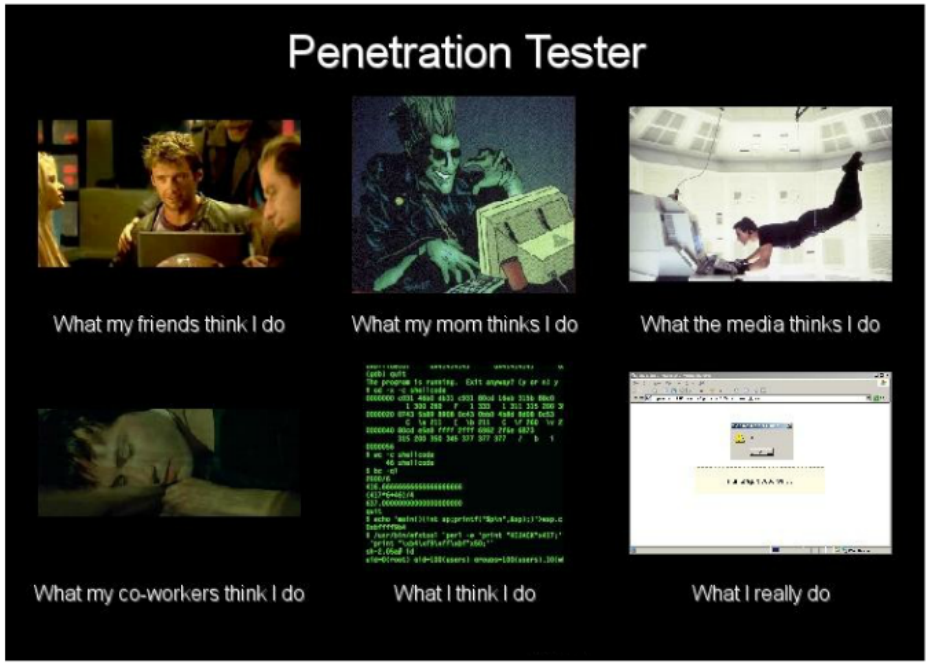
- we buy something but we don't configure it
- if we configure it, we dont' configure it properly
- if we configure it properly, we don't use them

↓

breach detected(?) after a month

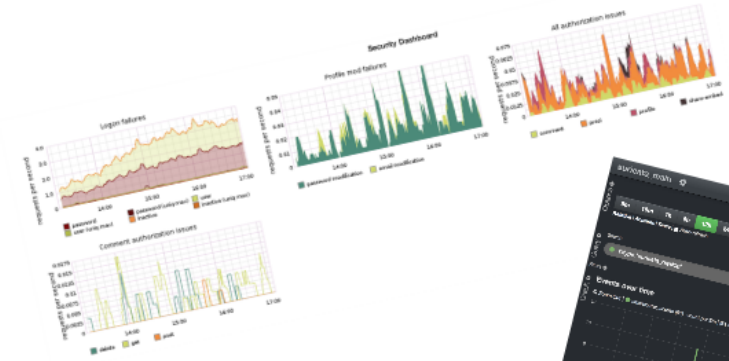
David Szili

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 dont' configure it properly
- if we configure it properly, we don't use them

breach detected(?) after a month

Blue team

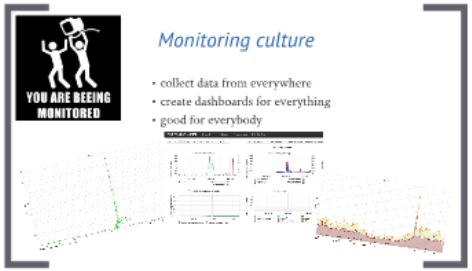
WTF is happening should not be a question!

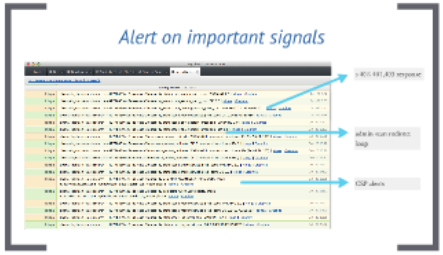
- centralized
- real time
- visual
- automated alerts

Don't just wait, be proactive!

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

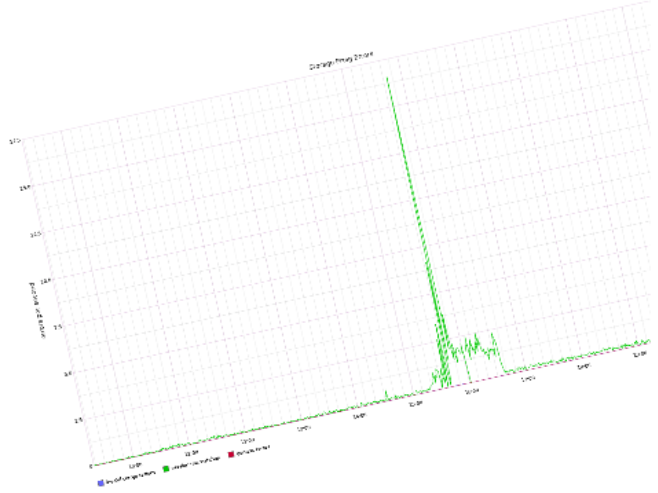
Monitoring & alerting

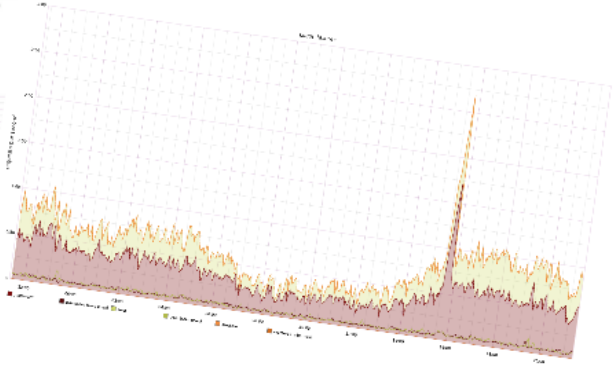




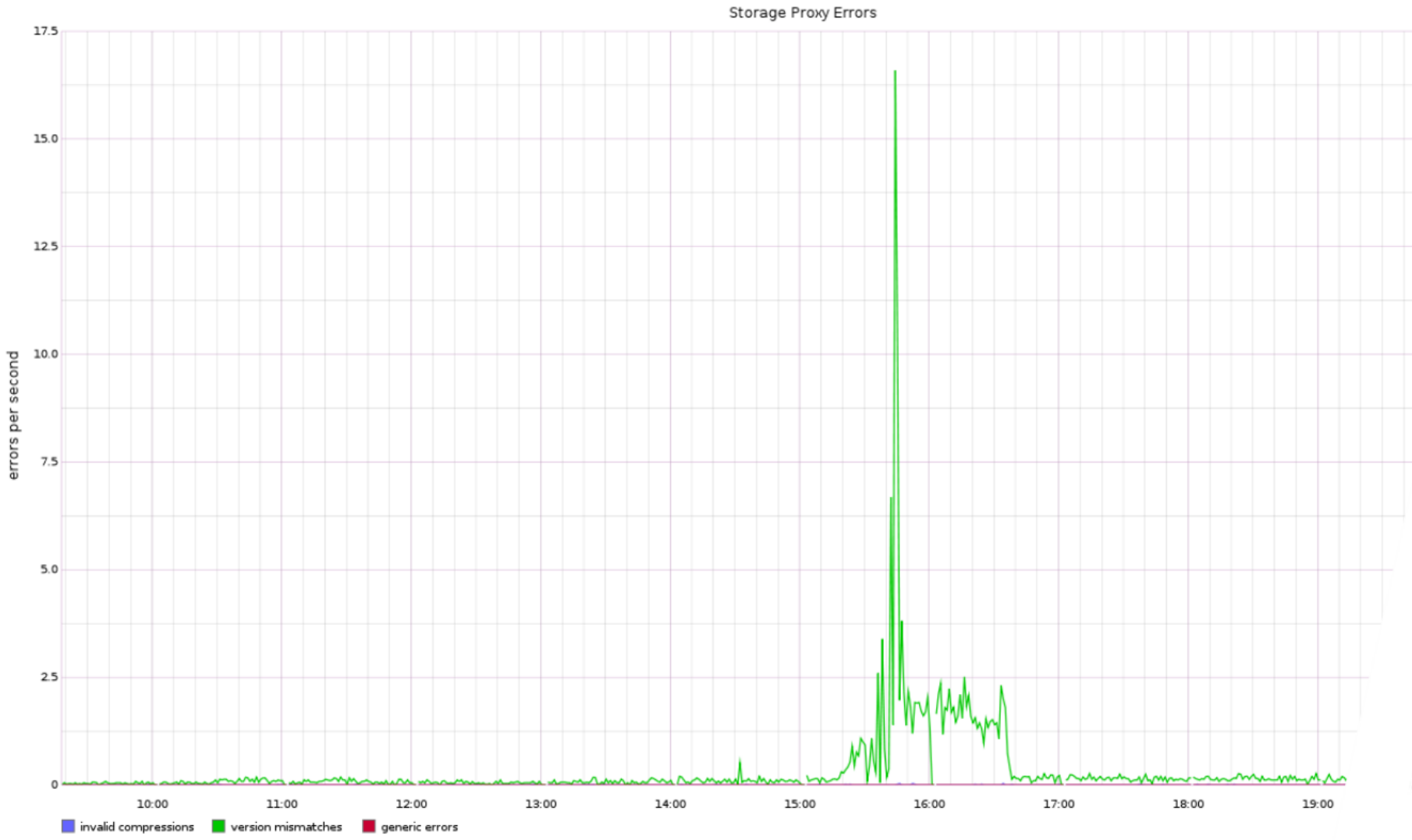
Monitoring culture

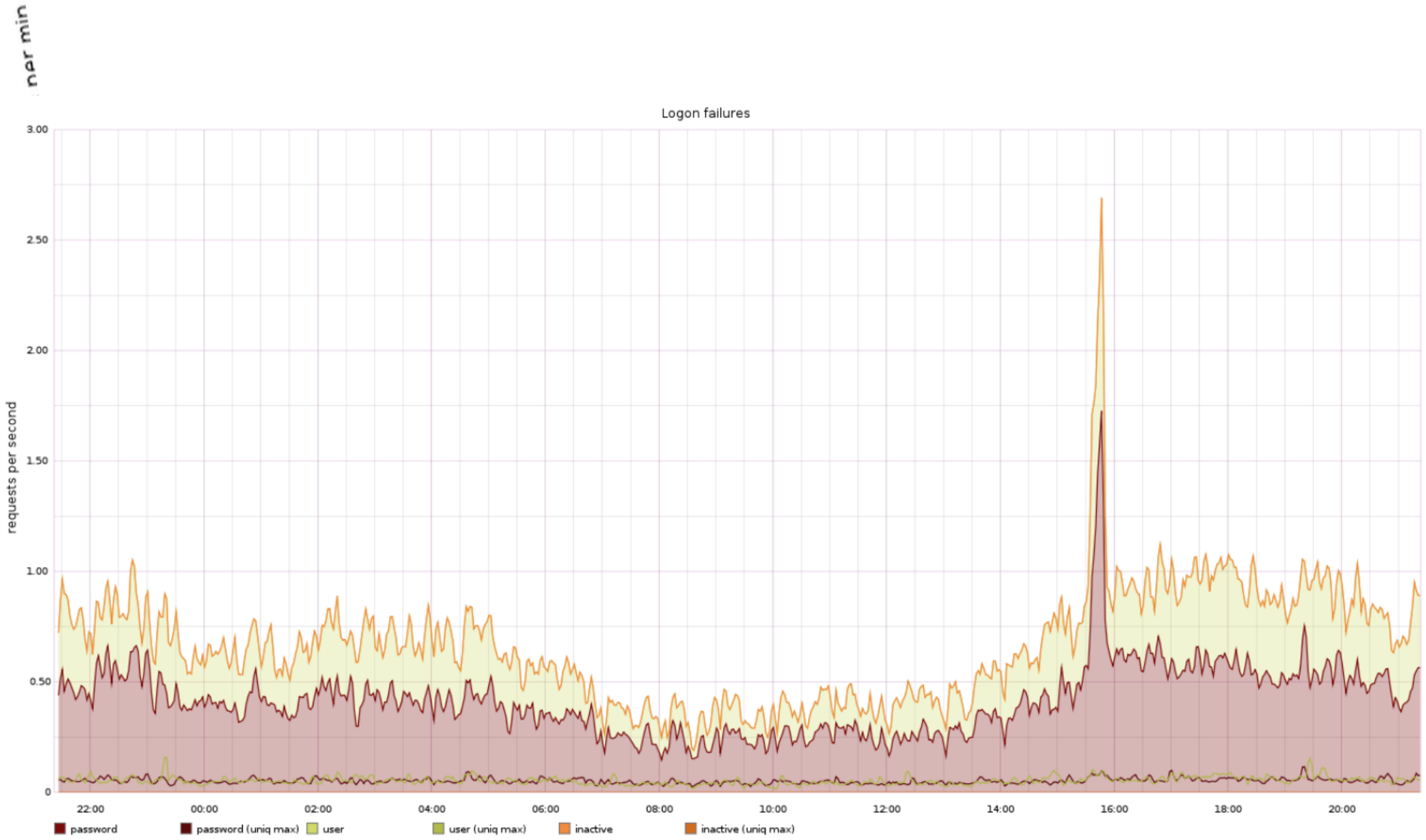
- collect data from everywhere
- create dashboards for everything
- good for everybody





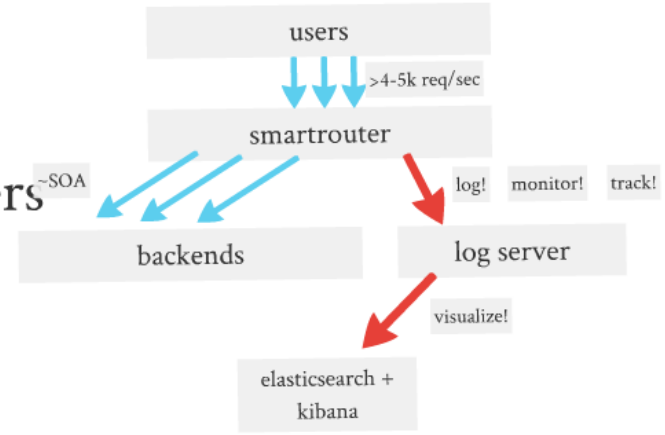
good for everybody

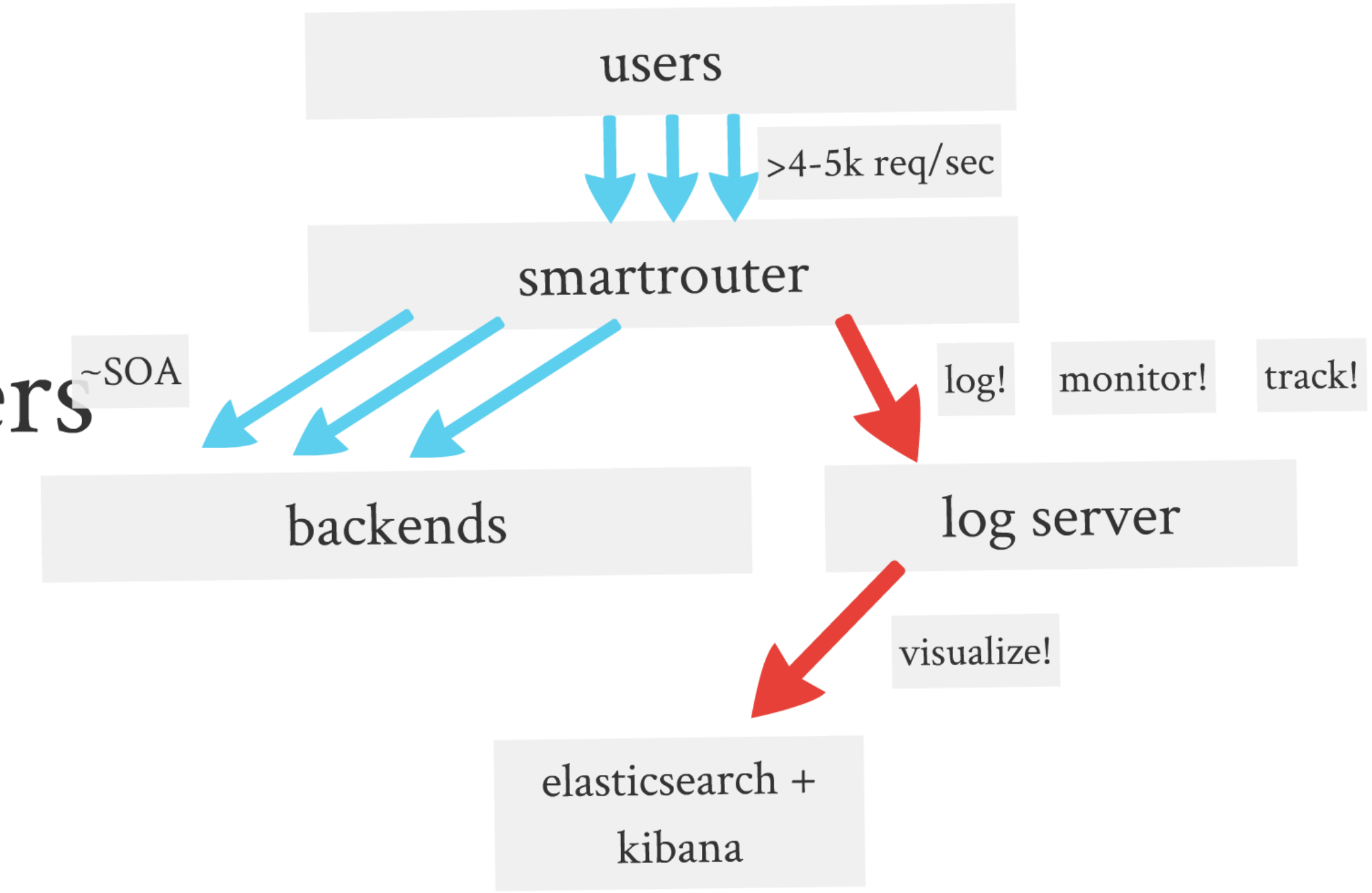

Storage Proxy Errors
errors per second
17.5
15.0
12.5
10.0
7.5
5.0
2.5
0
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
invalid compressions
version mismatches
generic errors


Logon failures
requests per second
3.00
2.50
2.00
1.50
1.00
0.50
0
22:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
password
password (uniq max)
user
user (uniq max)
inactive
inactive (uniq max)

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




users
>4-5k req/sec
smartrouter
~SOA
log!
monitor!
track!
backends
log server
visualize!
elasticsearch +
kibana

suricata_main

Kibana 3 milestone pre-3

Options

5m | 15m | 1h | 6h | 12h | 24h | 2d | 7d | 30d

Relative | Absolute | Since | Auto-refresh

Dashboard Control

Query

Search

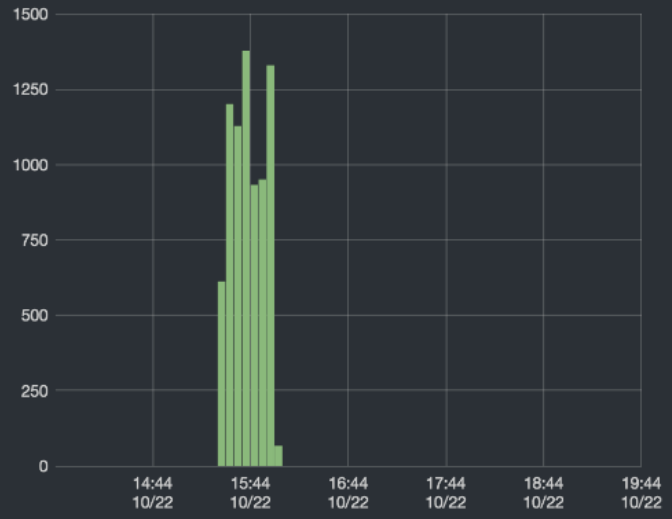
@type:"suricata_rsyslog"

Filters

Graph

Events over time

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



source ips

Term	Count	Action
87.68.38.93	7454	
220.244.133.152	92	
172.30.1.244	6	
172.30.1.243	4	
172.30.1.246	3	
172.30.1.245	1	

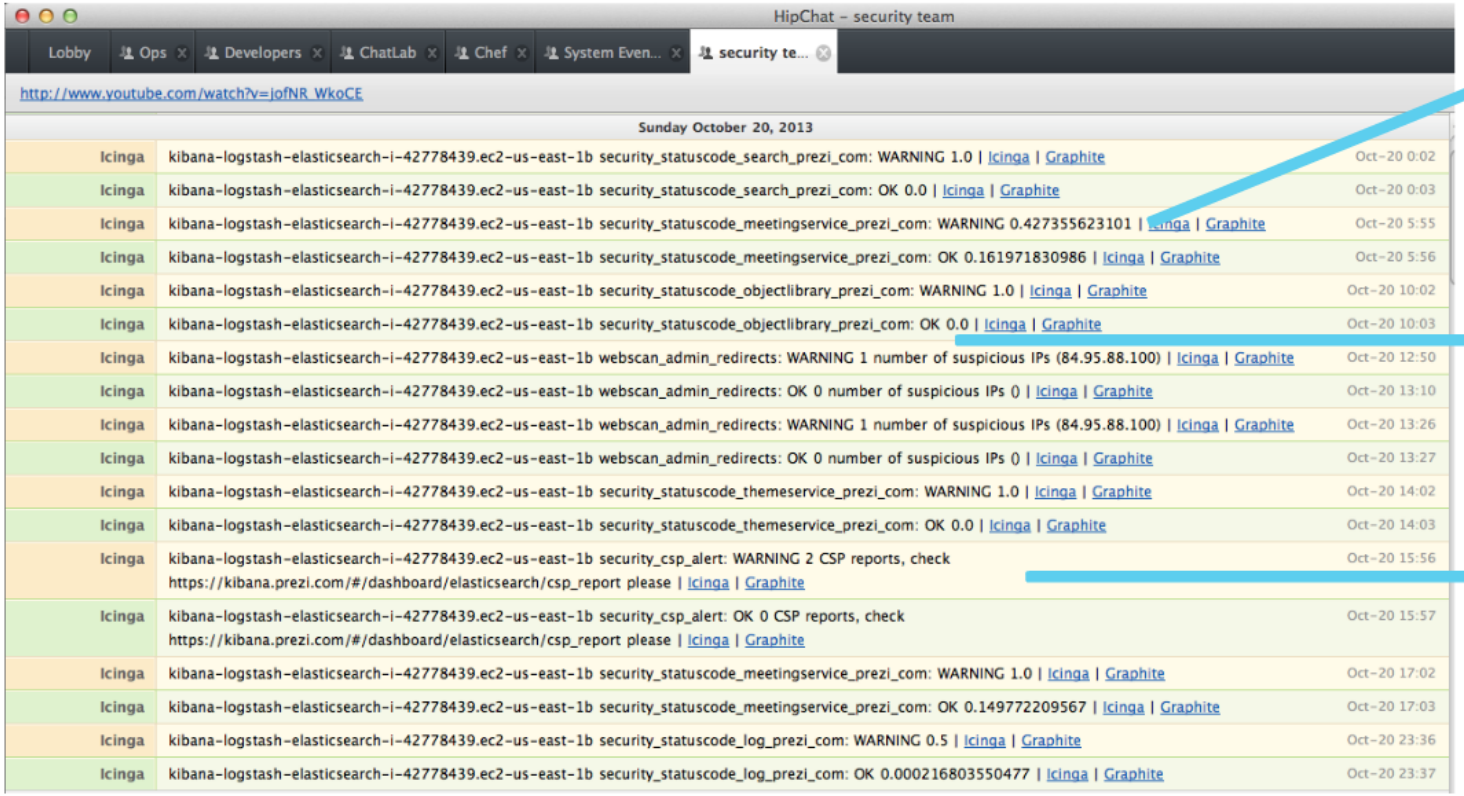
top attack types

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

least common attacks

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

Alert on important signals



>40% 401,403 response

admin scan redirect loop

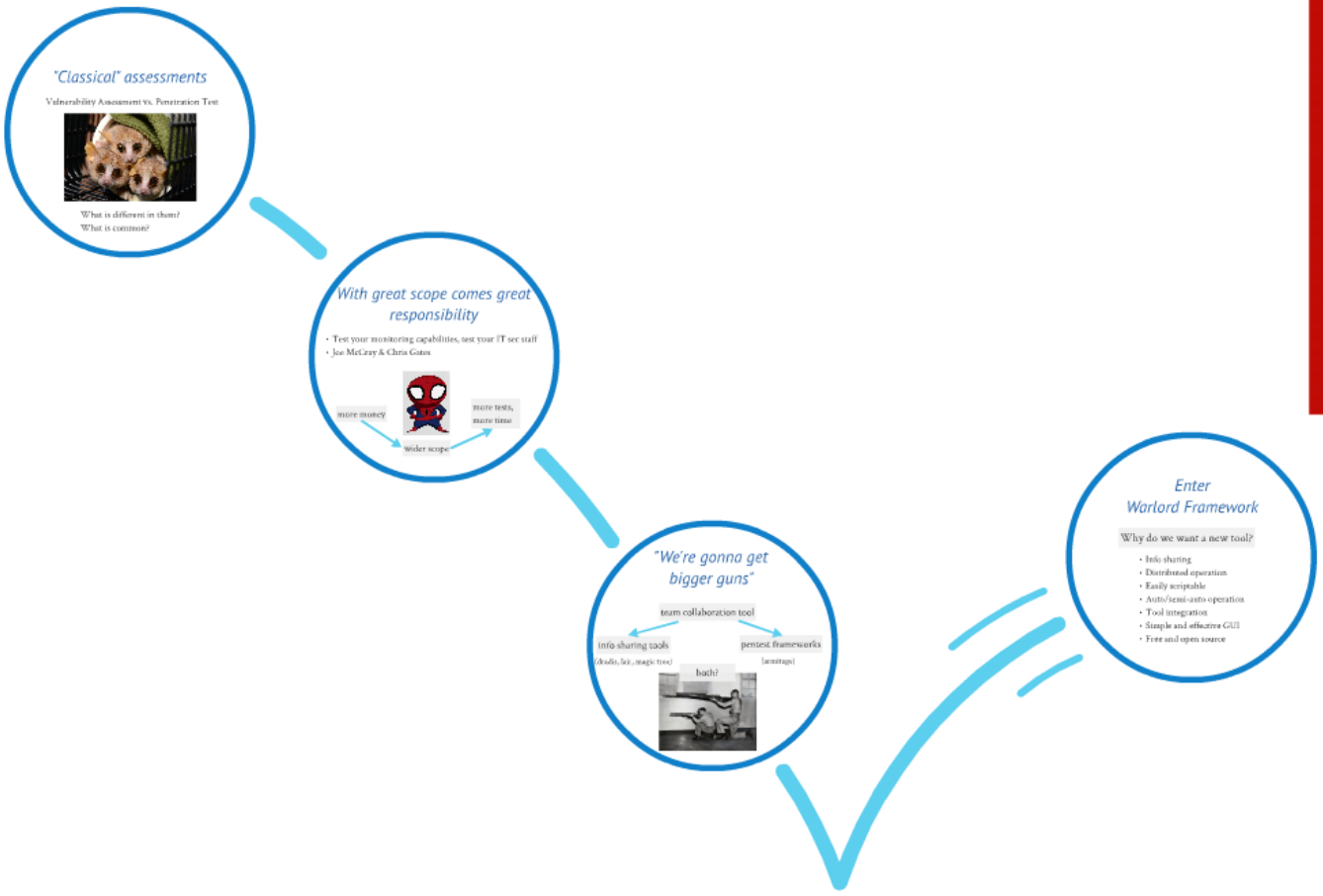
CSP alerts


slow them down
detect them
identify them
VIA 9GAG.COM

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
wider scope
more tests, more time
"We're gonna get bigger guns"
team collaboration tool
info sharing tools
(dradis, fair, 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


KEEP
CALM
the
RED TEAM
IS HERE

"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

wider scope

more tests,
more time

"We're gonna get bigger guns"

team collaboration tool

info sharing tools

(dradis, lair, magic tree)

pentest frameworks

(armitage)

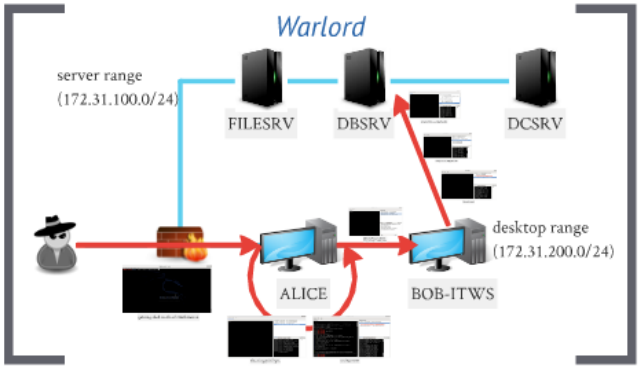
both?

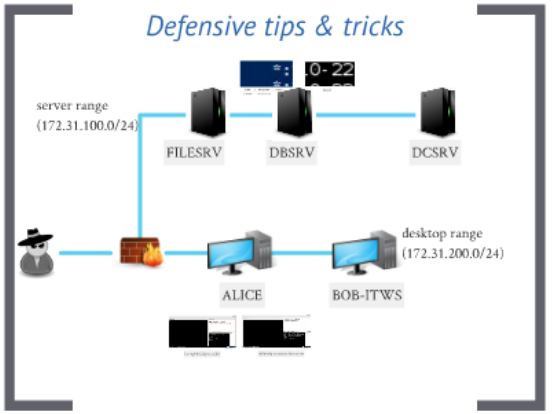
Enter Warlord Framework

Why do we want a new tool?

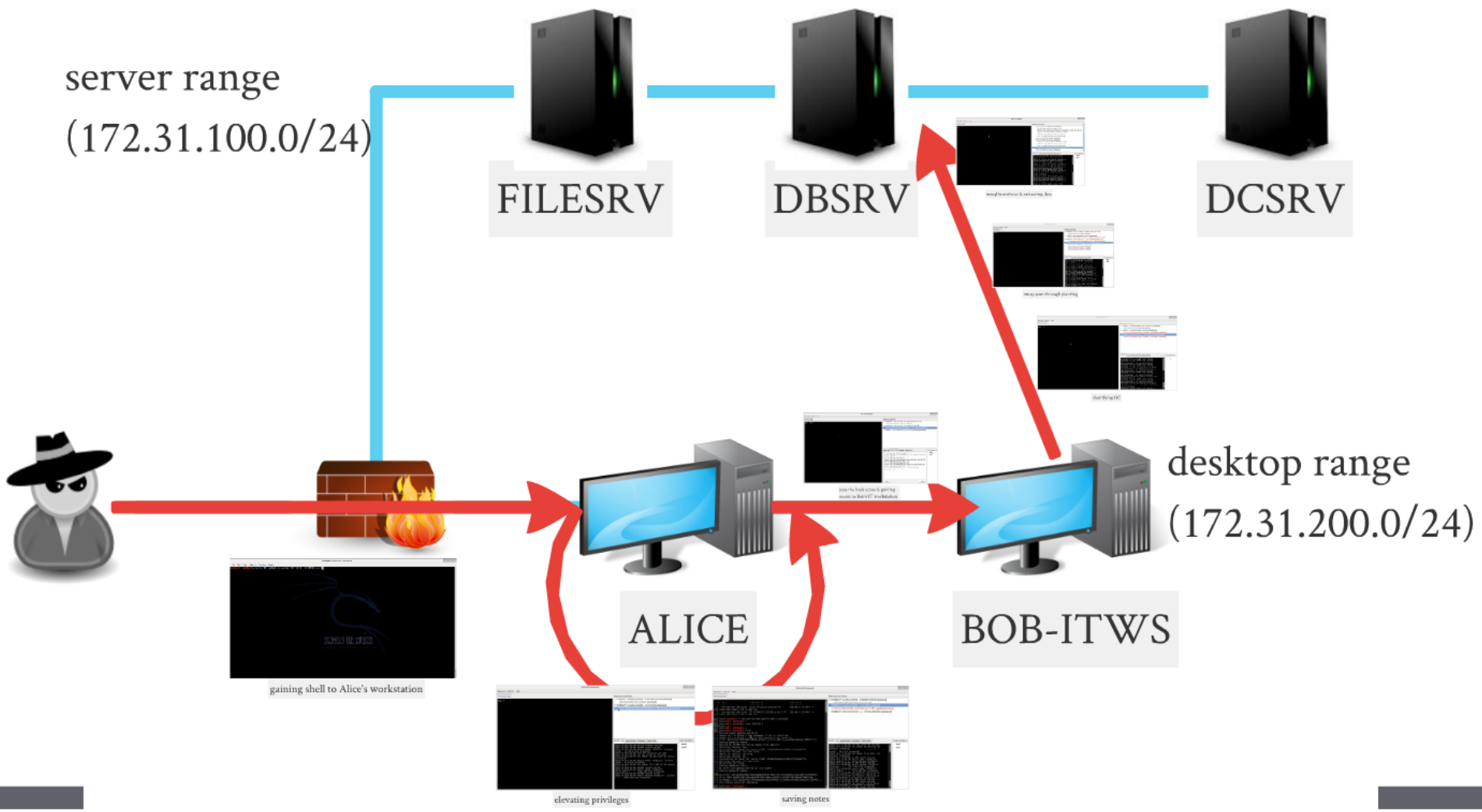
- Info sharing
- Distributed operation
- Easily scriptable
- Auto/semi-auto operation
- Tool integration
- Simple and effective GUI
- Free and open source

Enough talkin'



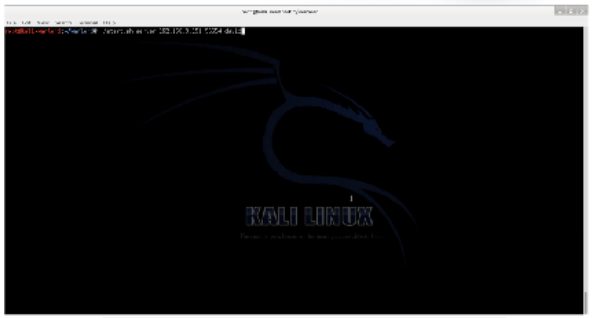


Warlord


server range
(172.31.100.0/24)
FILESRV
DBSRV
DCSRV
desktop range
(172.31.200.0/24)
ALICE
BOB-ITWS
gaining shell to Alice's workstation
elevating privileges
saving notes

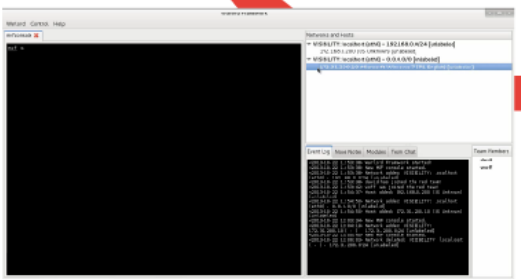
FILESRV

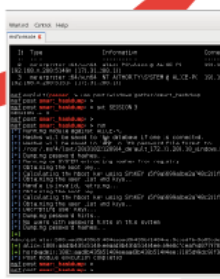
D



gaining shell to Alice's workstation

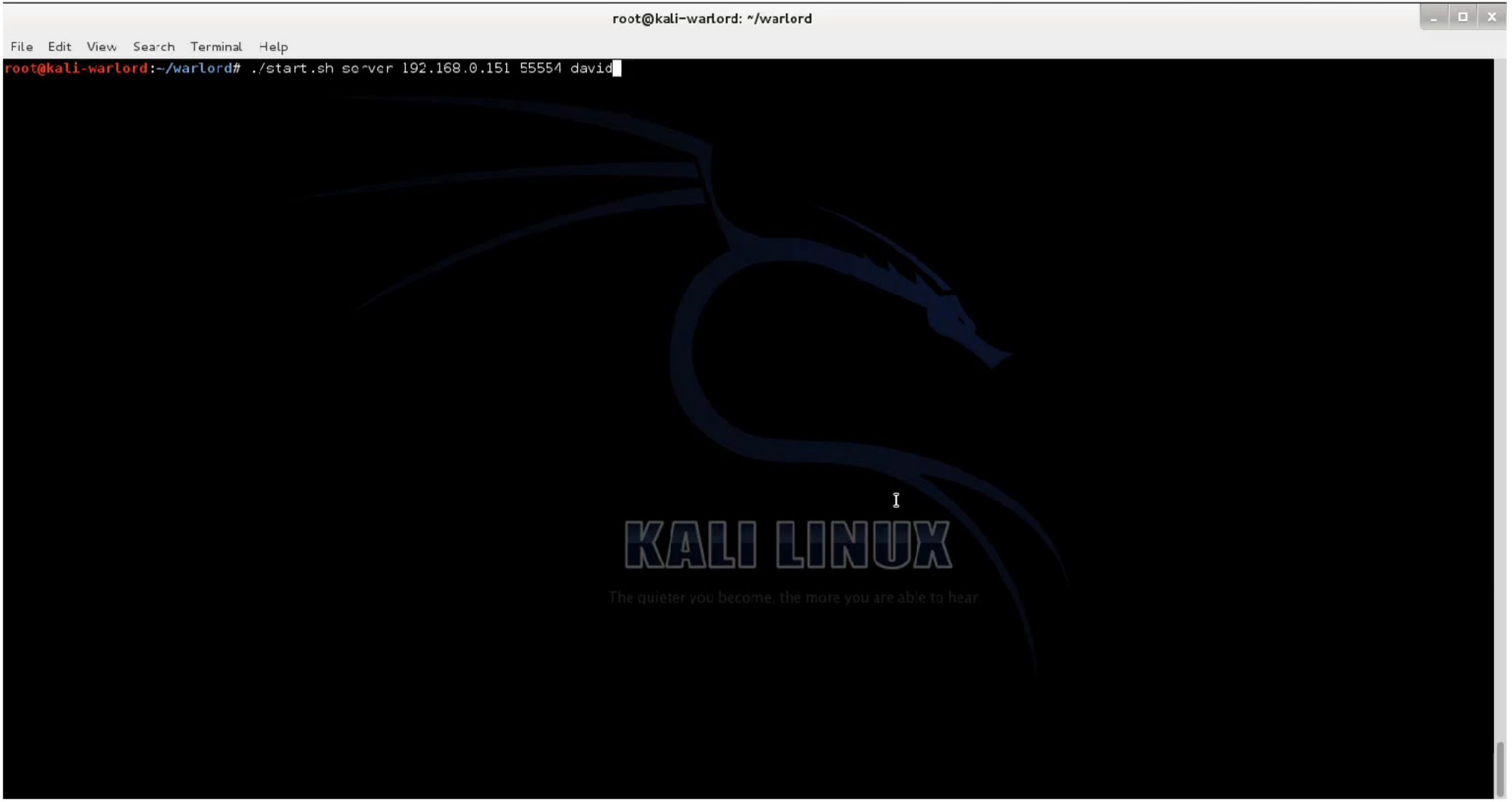
ALICE



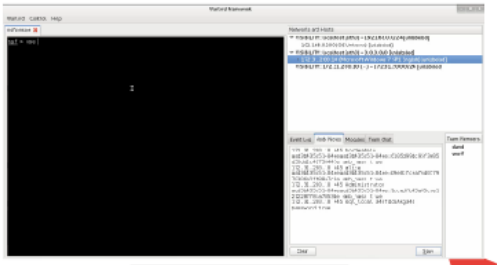


elevating privileges

savi



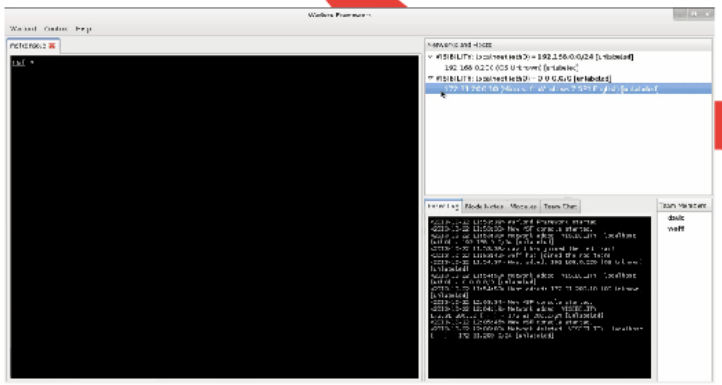
gaining shell to Alice's workstation



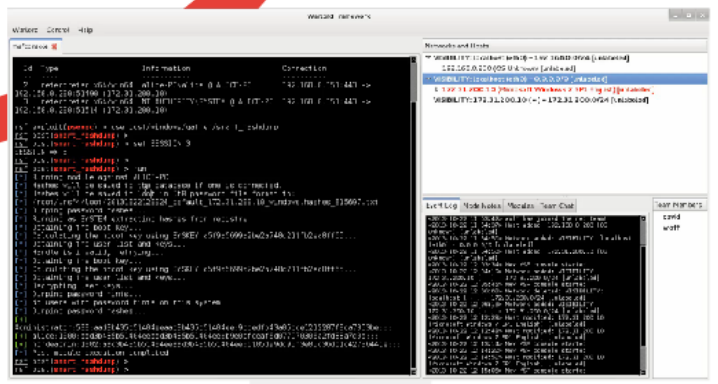
pass the hash scans & gaining access to Bob's IT workstation

ALICE

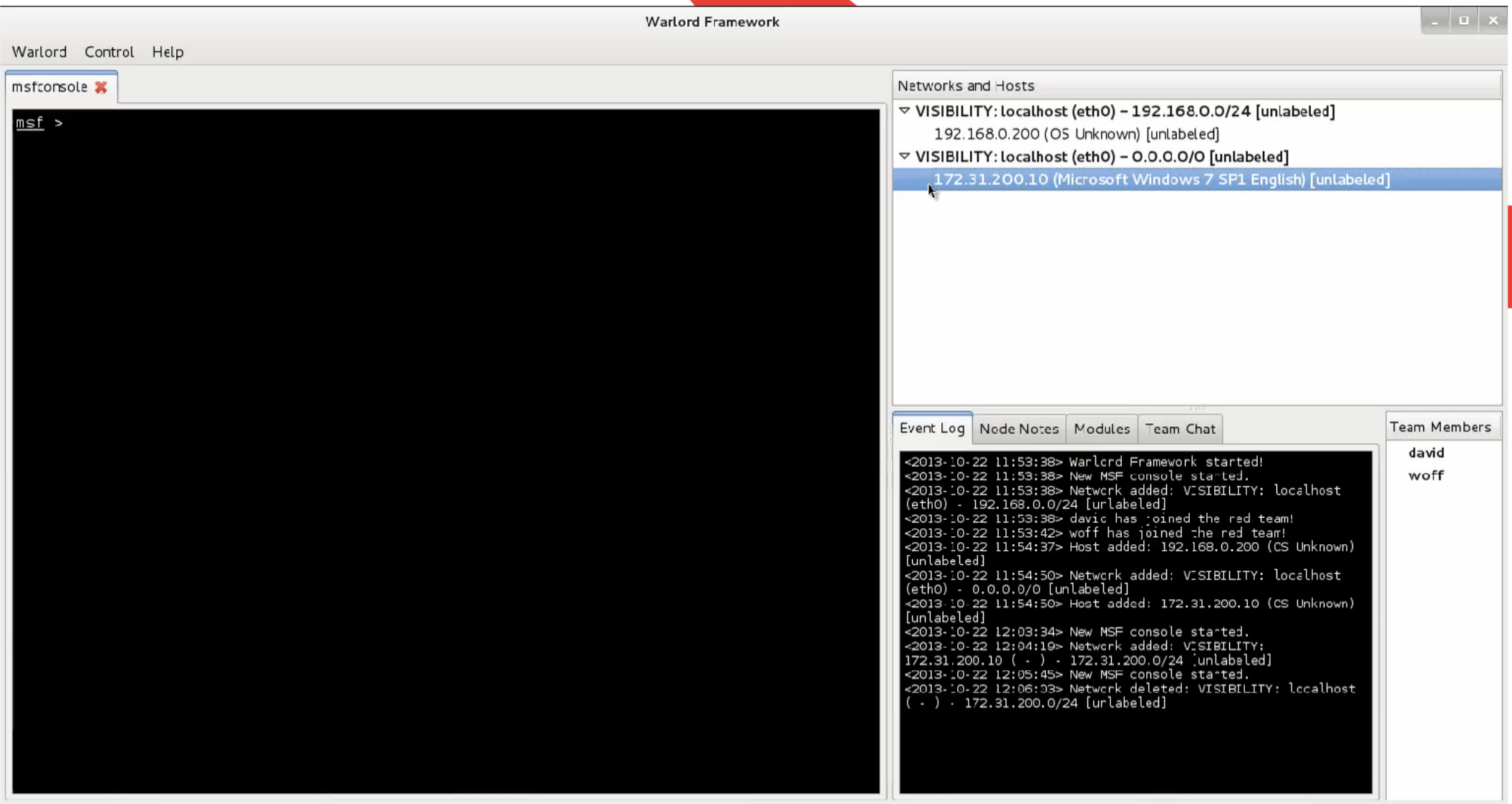
BO



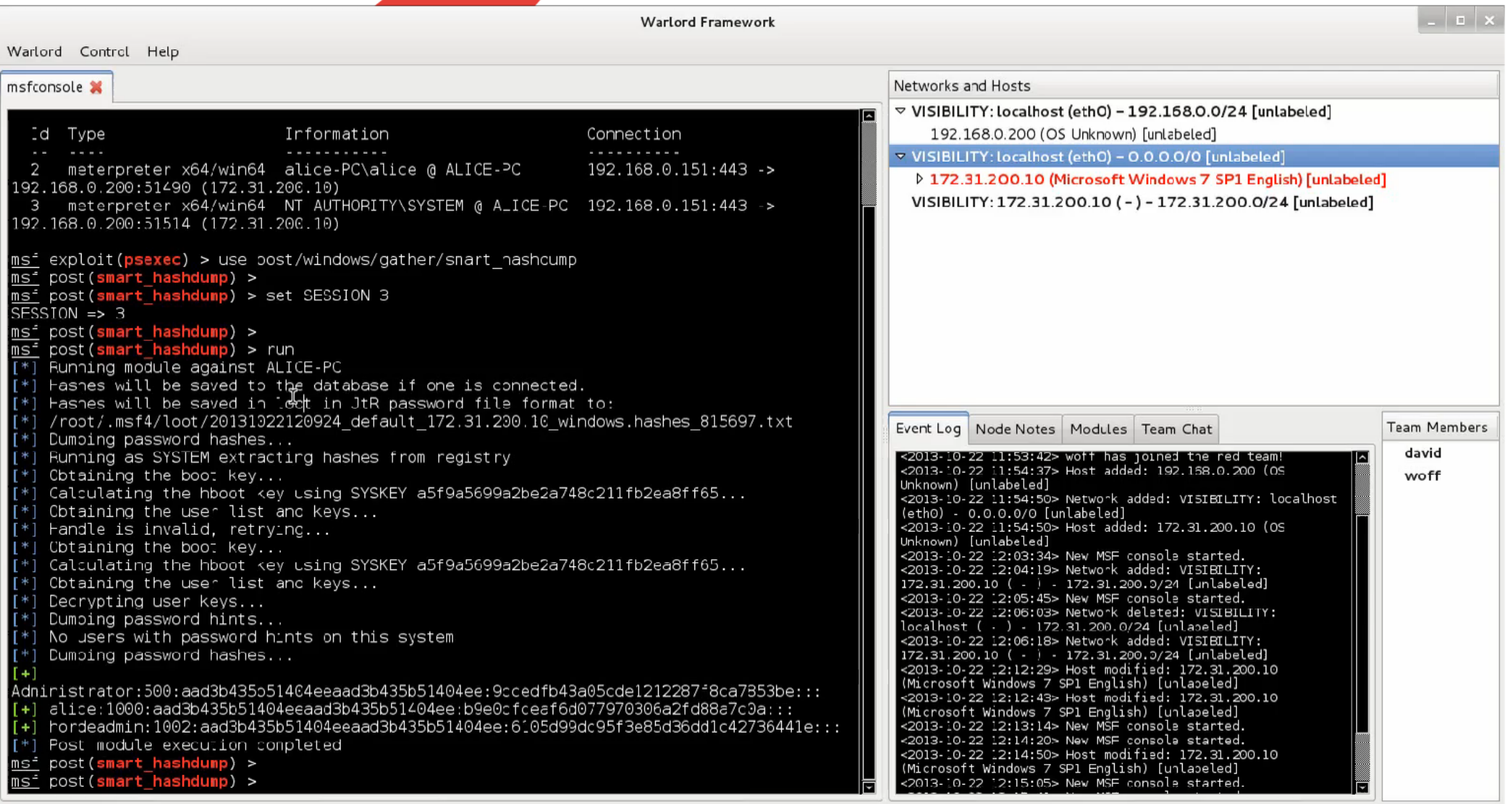
elevating privileges



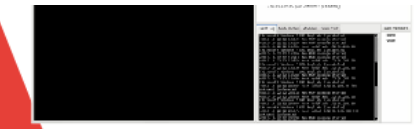
saving notes



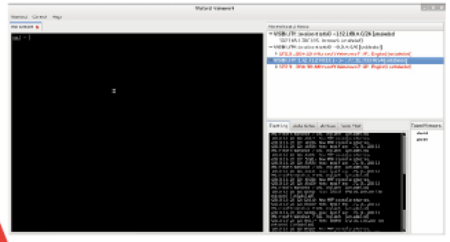
elevating privileges



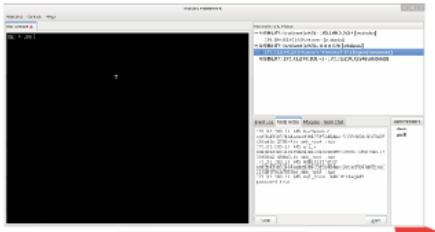
saving notes



nmap scan through pivoting



identifying DC



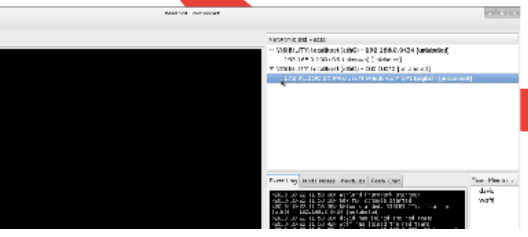
pass the hash scans & gaining
access to Bob's IT workstation

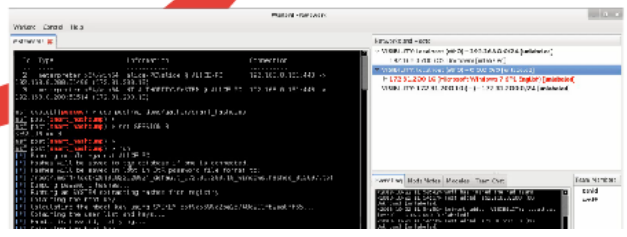
ALICE

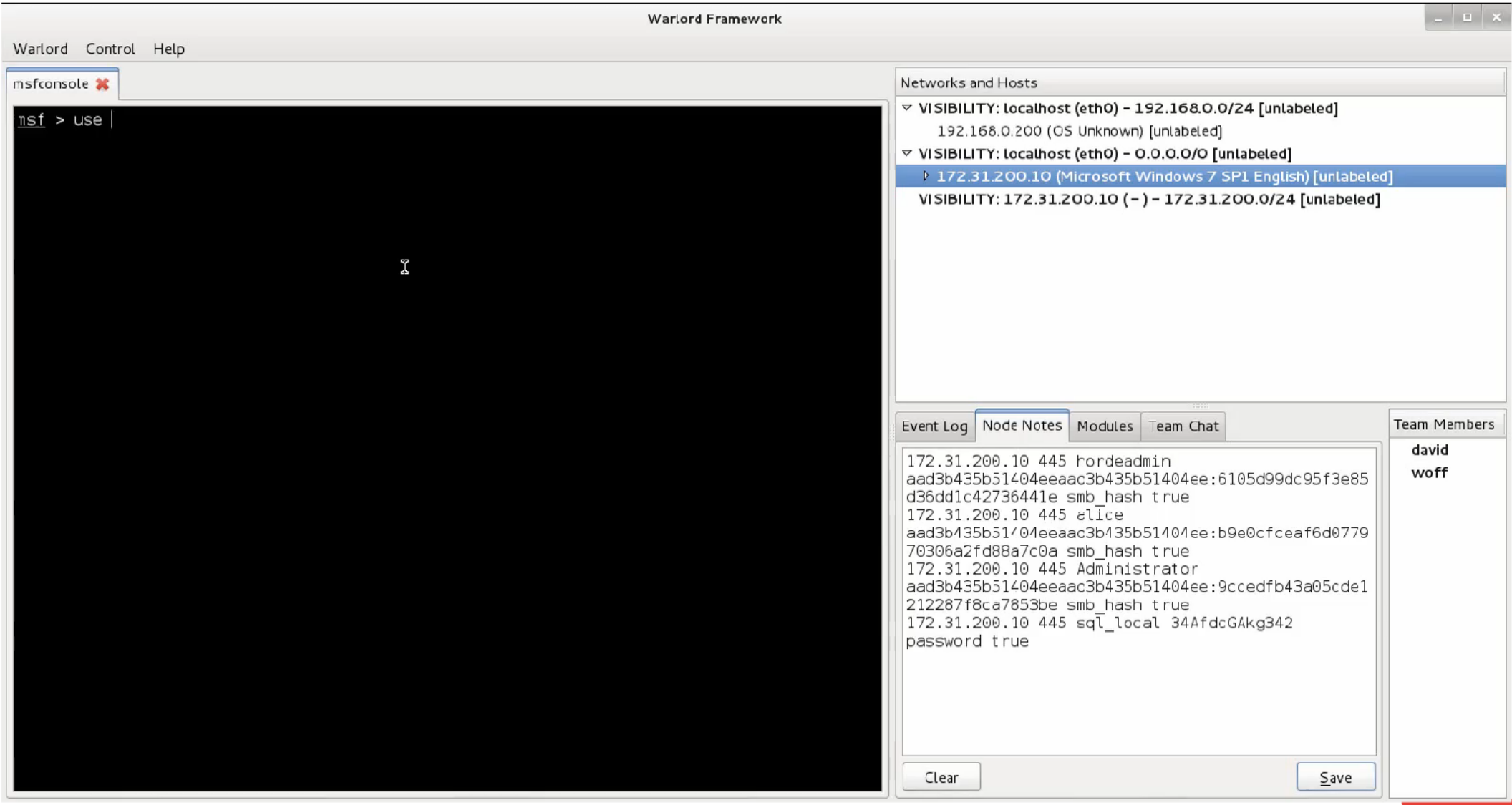
BOB-ITWS

de

(1

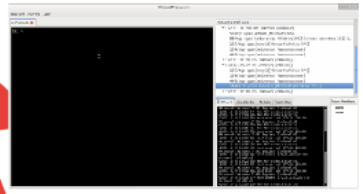




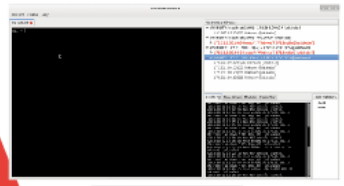


pass the hash scans & gaining access to Bob's IT workstation

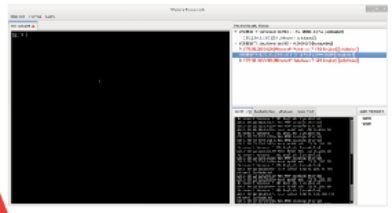
DBSRV



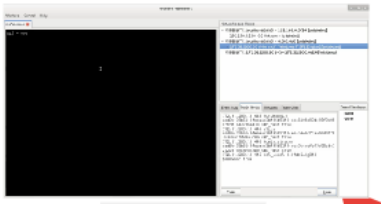
mssql bruteforce & extracting data



nmap scan through pivoting



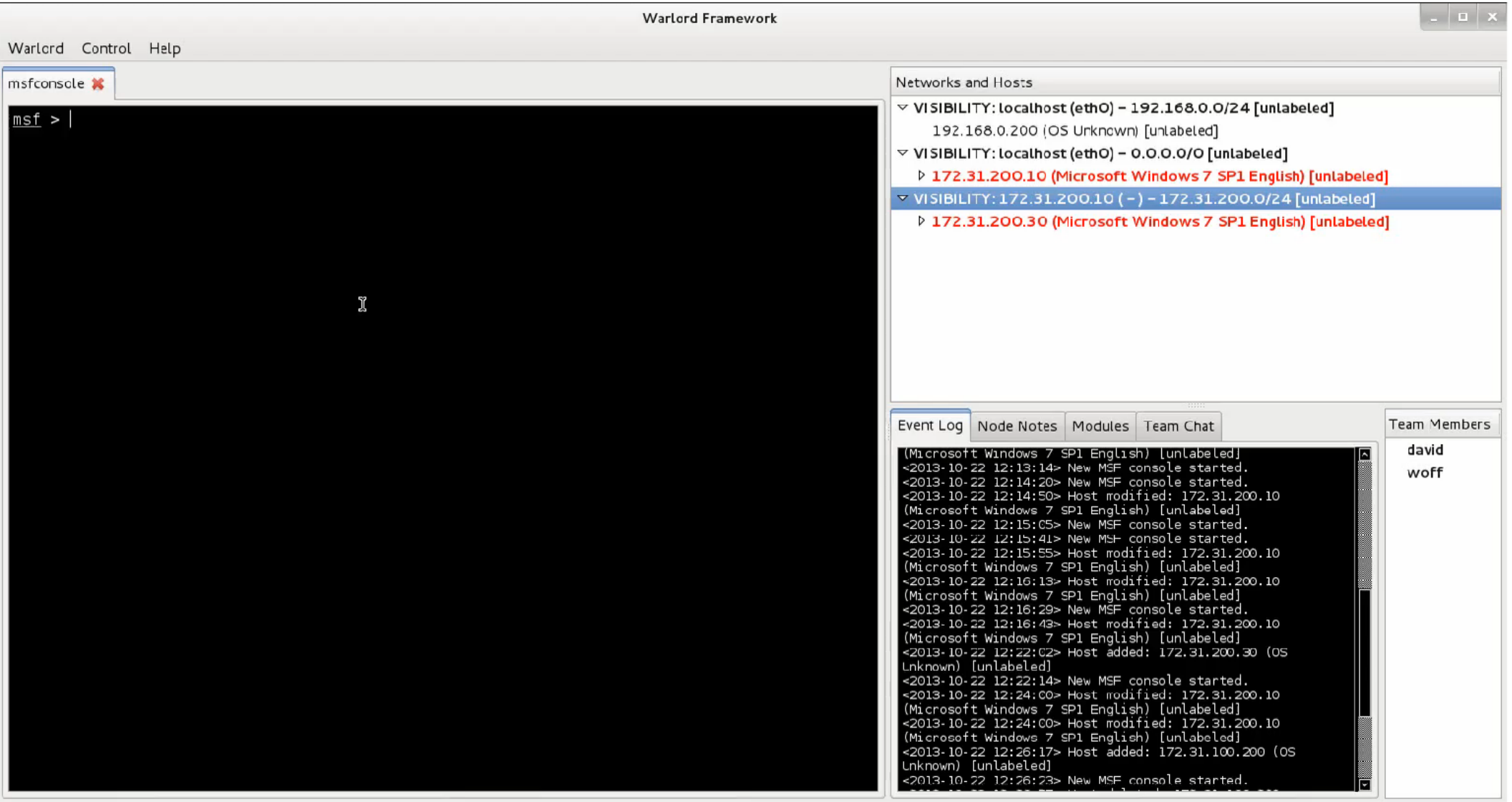
identifying DC



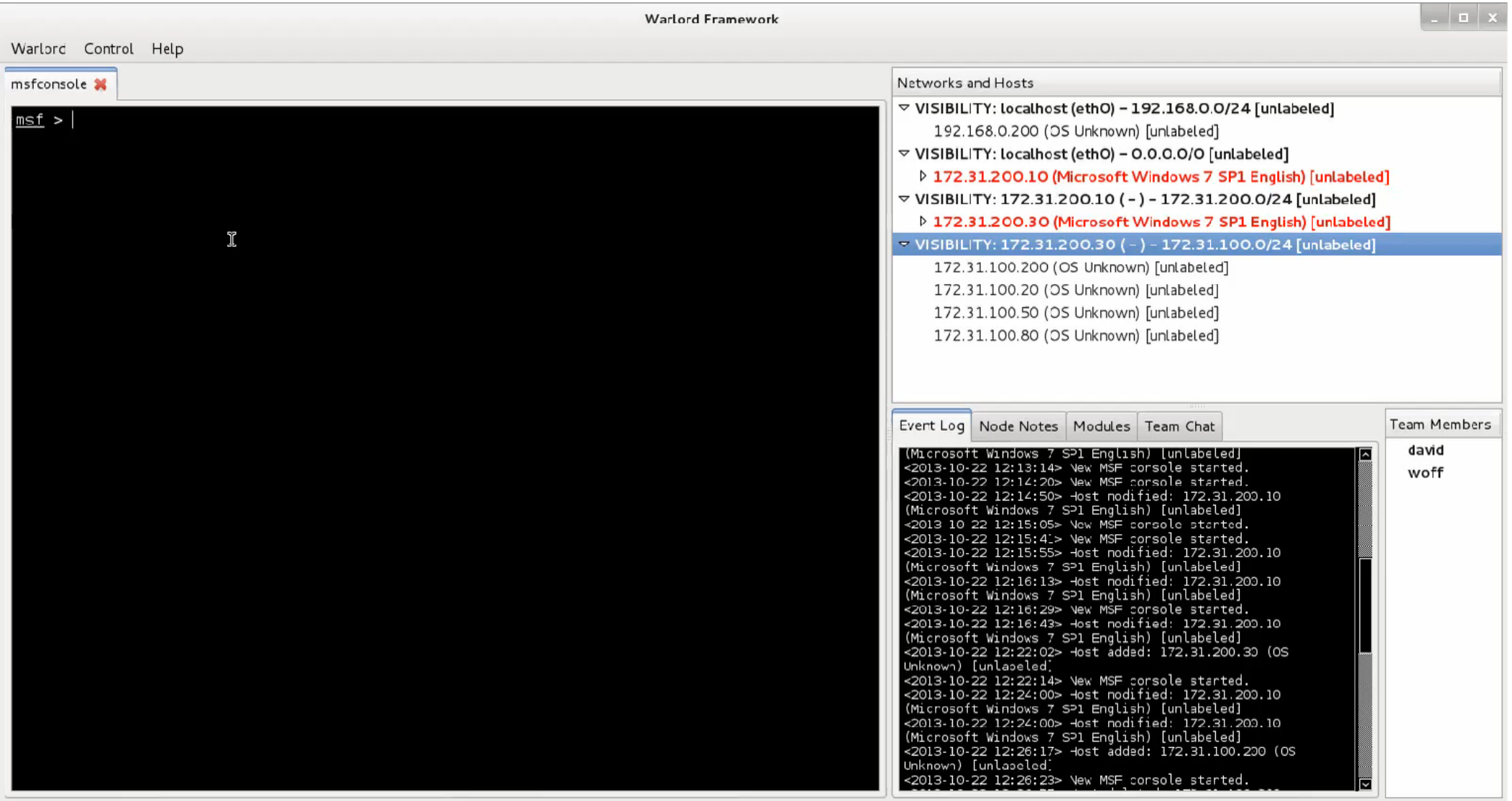
pass the hash scans & gaining access to Bob's IT workstation

DCSRV

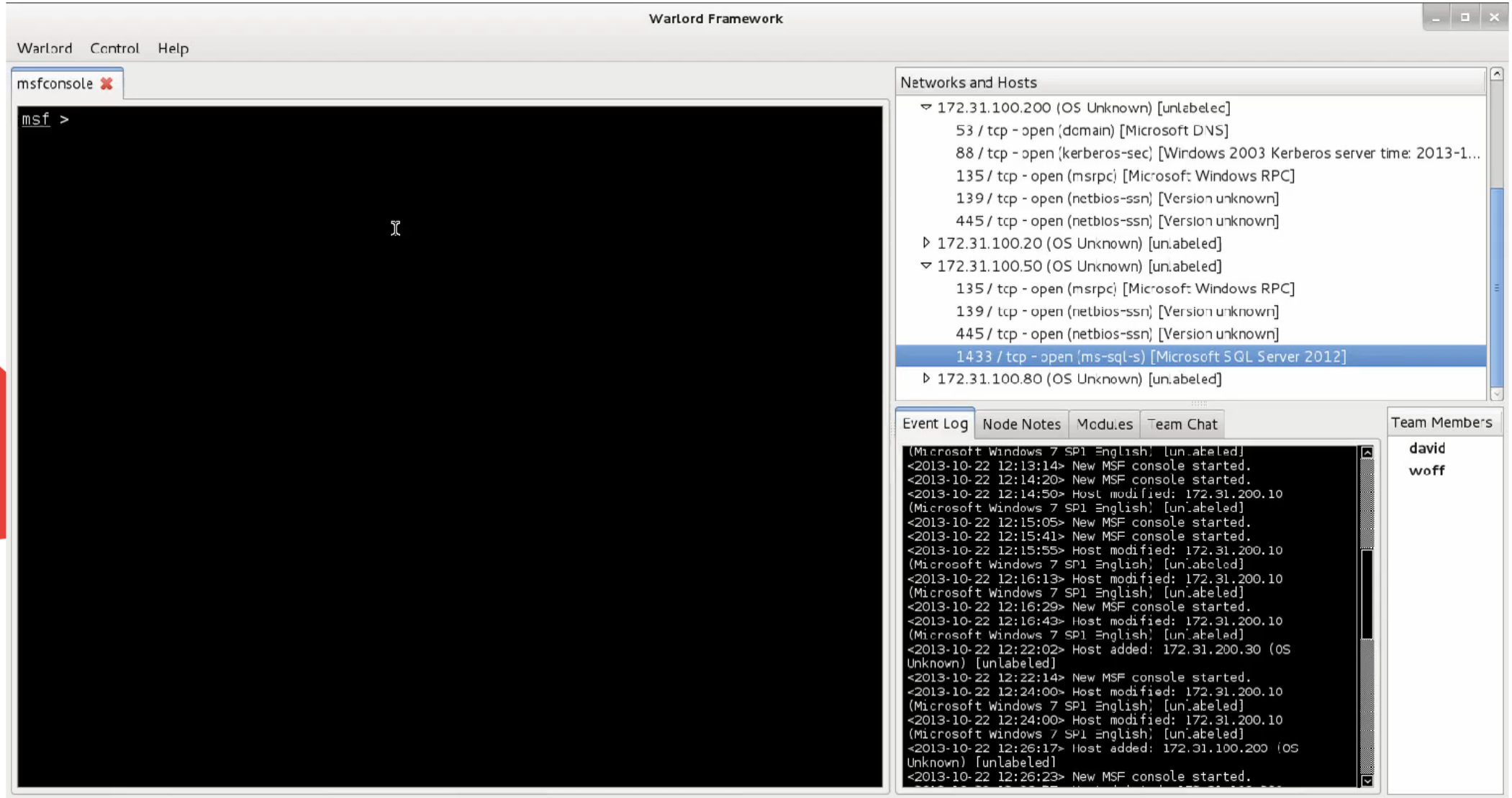
desktop range (172.31.200.0/24)



identifying DC

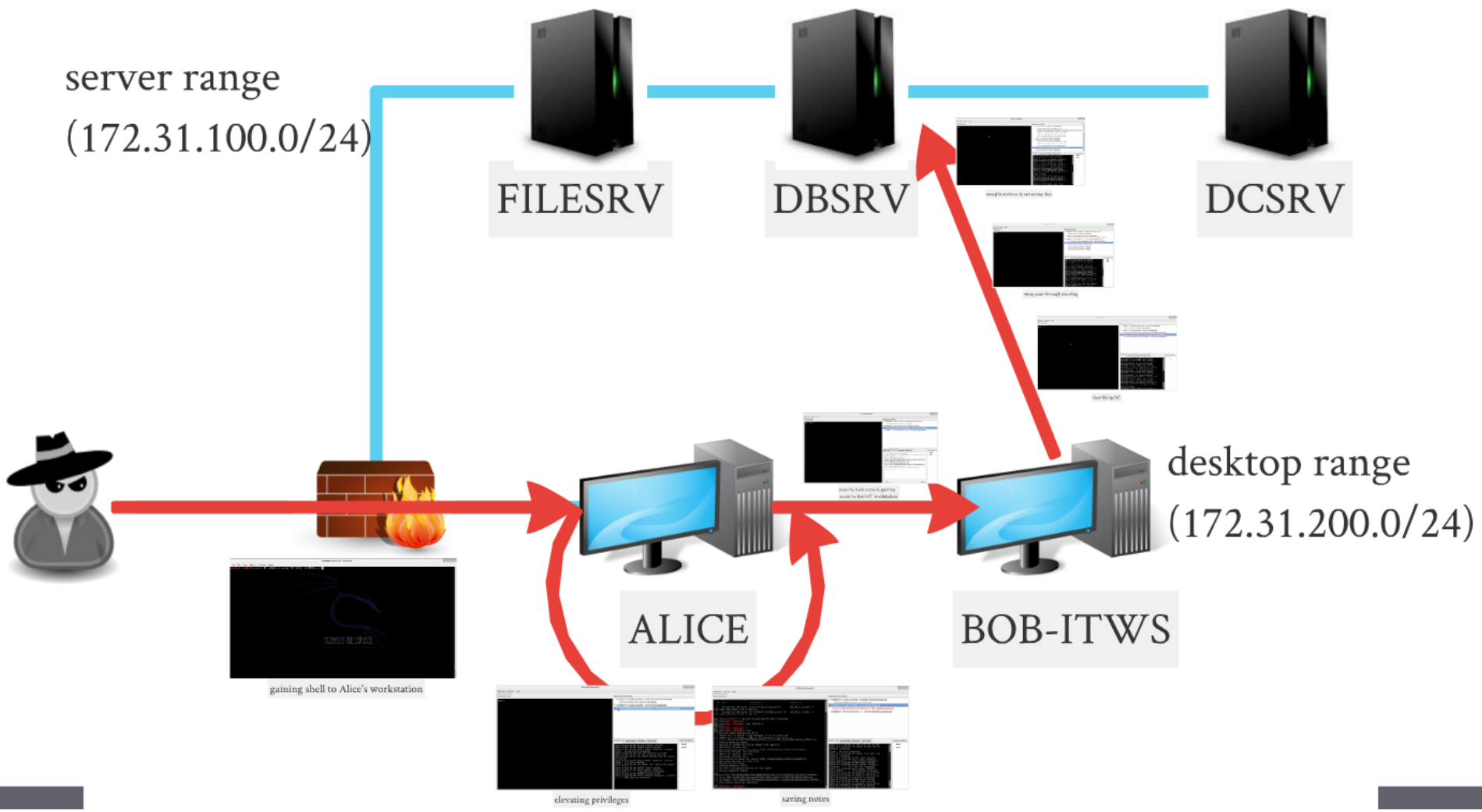


nmap scan through pivoting

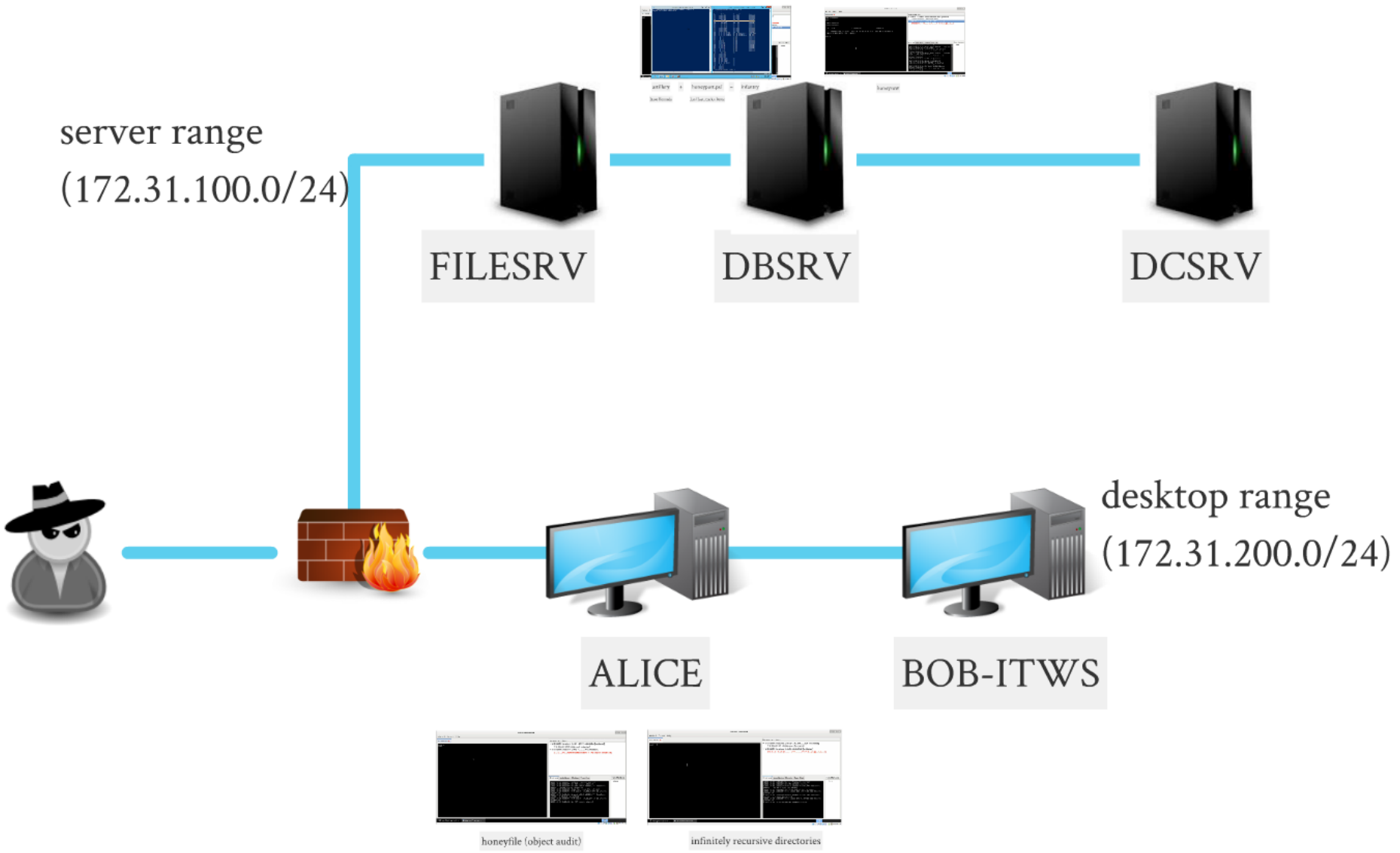


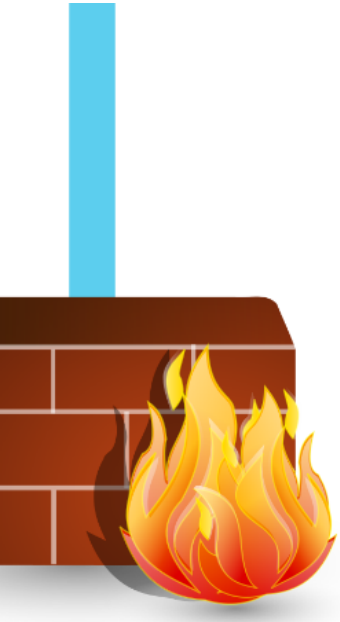
mssql bruteforce & extracting data

Warlord

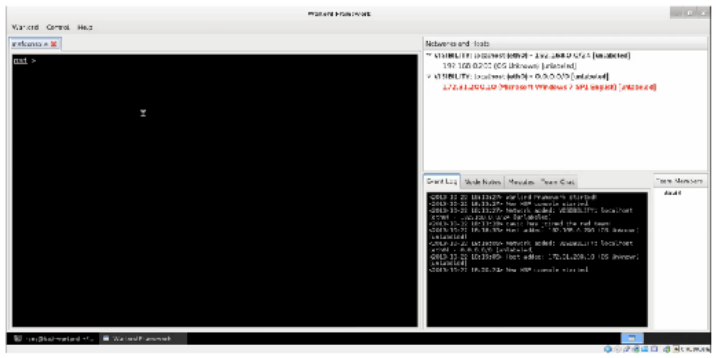

server range
(172.31.100.0/24)
FILESRV
DBSRV
DCSRV
desktop range
(172.31.200.0/24)
ALICE
BOB-ITWS
gaining shell to Alice's workstation
elevating privileges
saving notes

Defensive tips & tricks

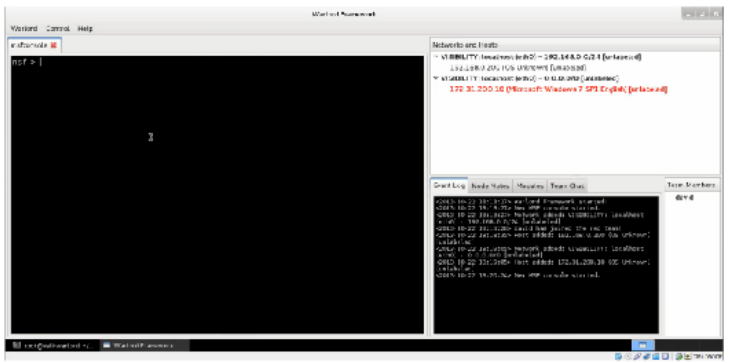




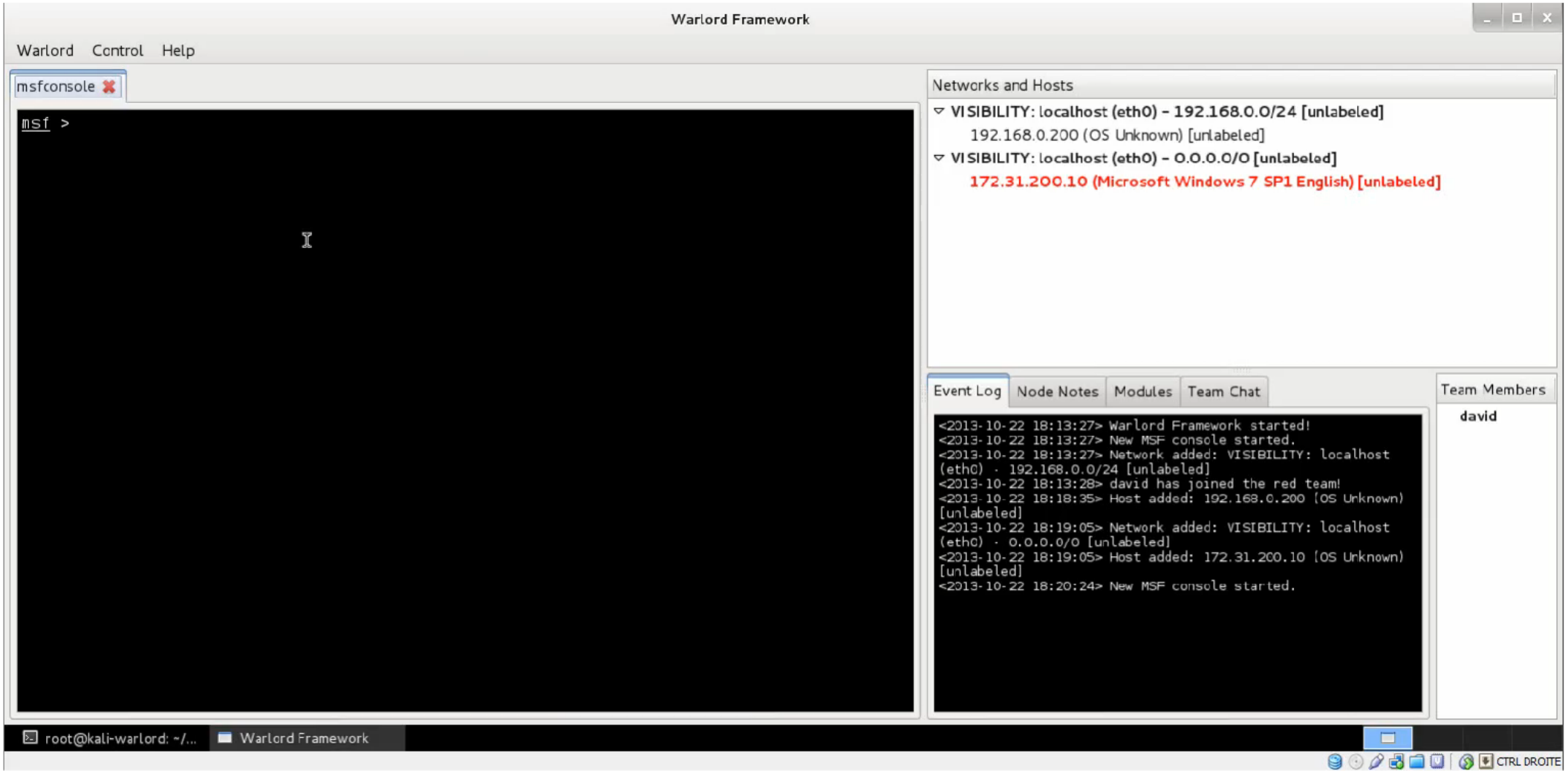
ALICE



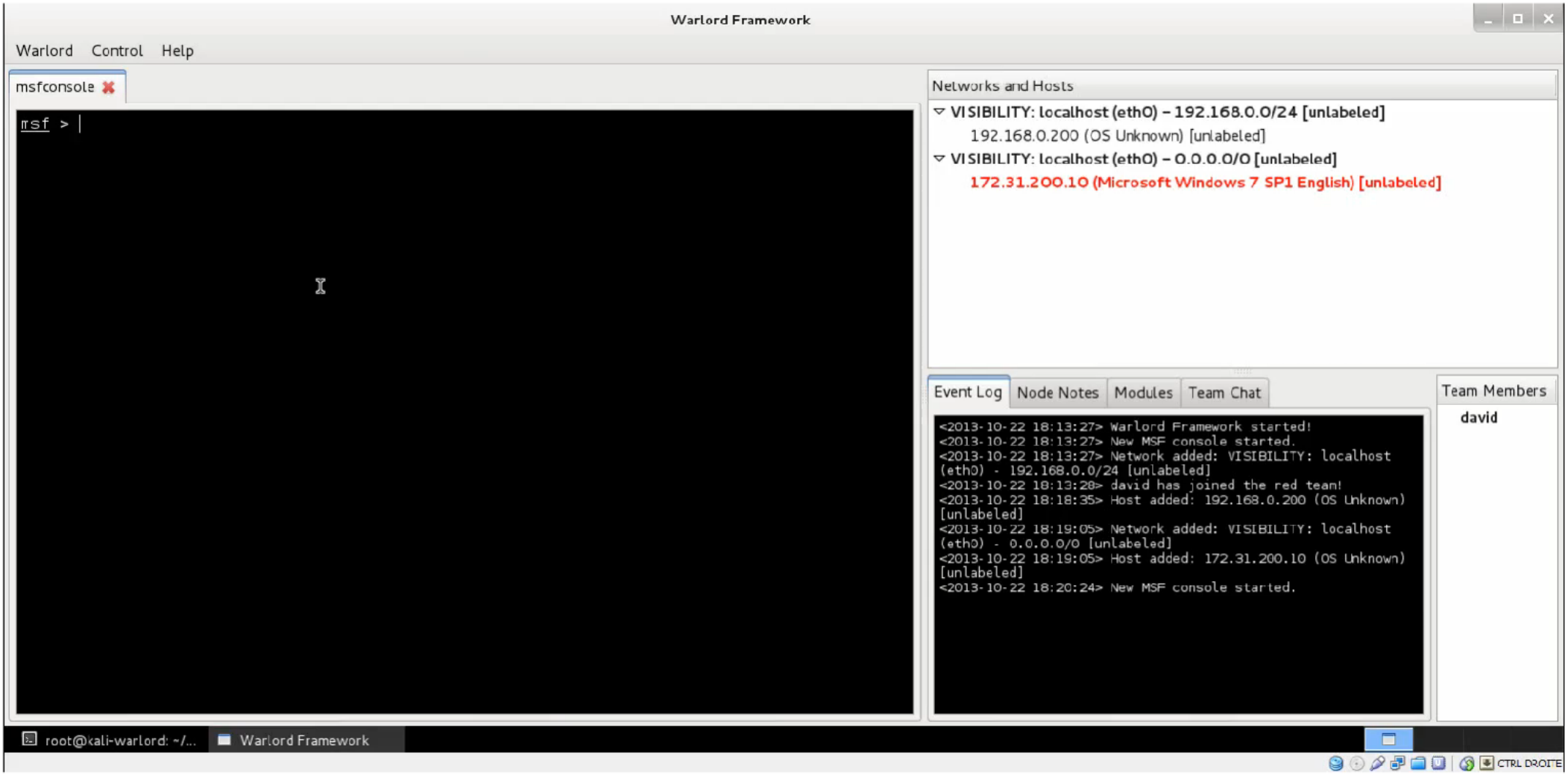
honeyfile (object audit)



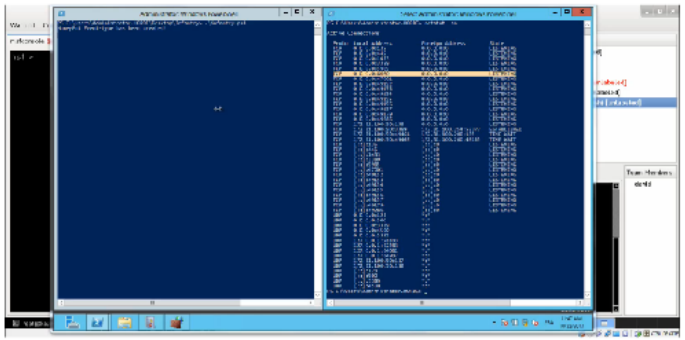
infinitely recursive directories

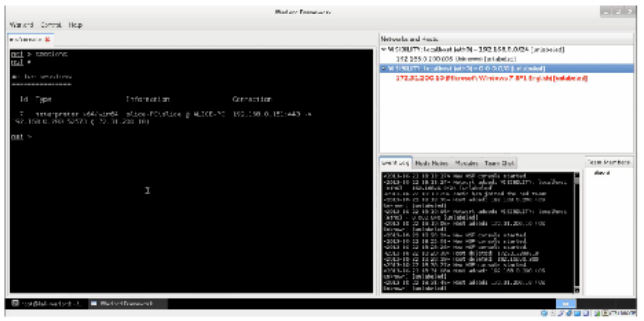


honeyfile (object audit)



infinitely recursive directories



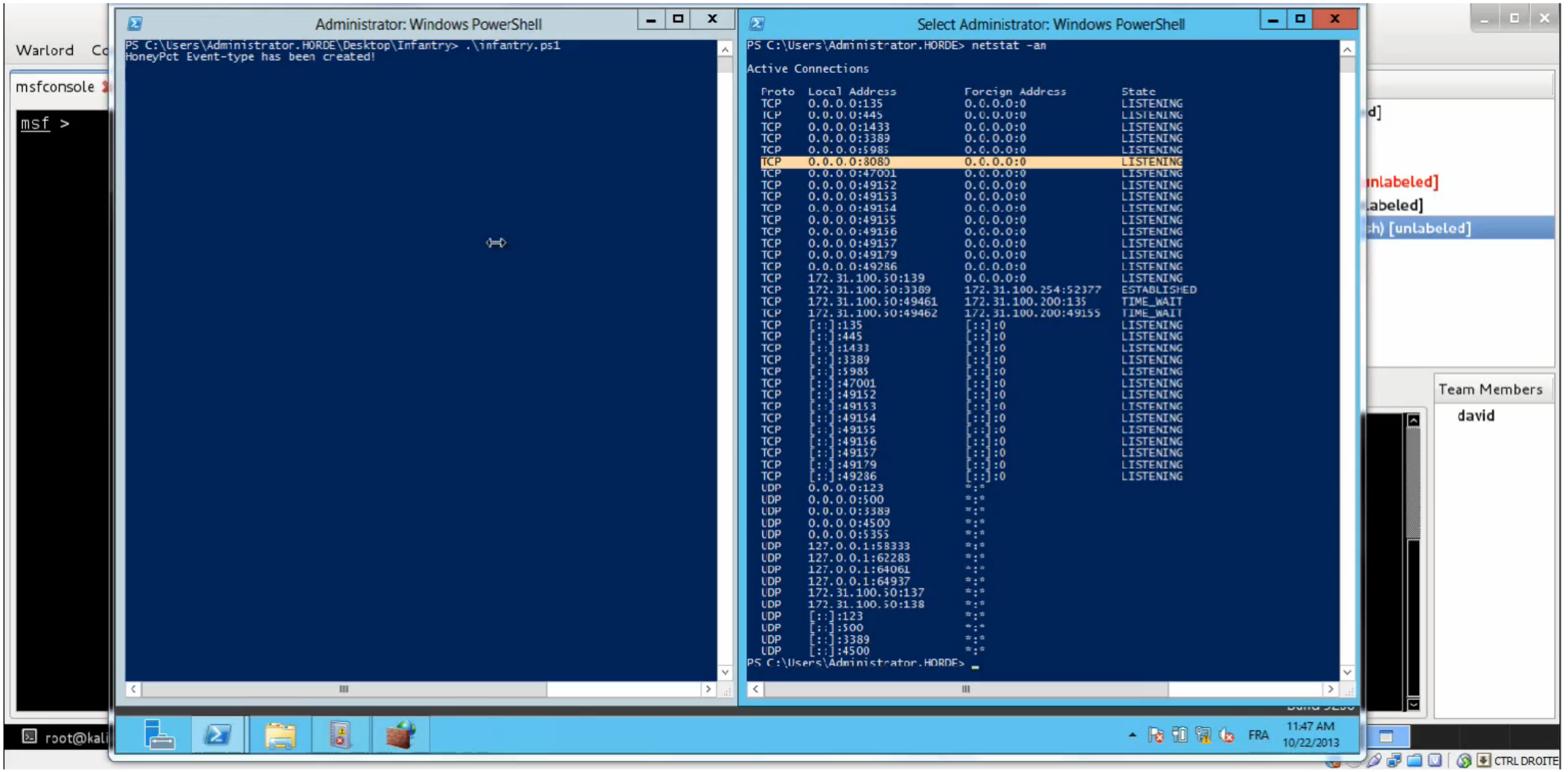


artillery + honeyport.ps1 = infantry

Dave Kennedy — Jon Hoyt, Carlos Perez

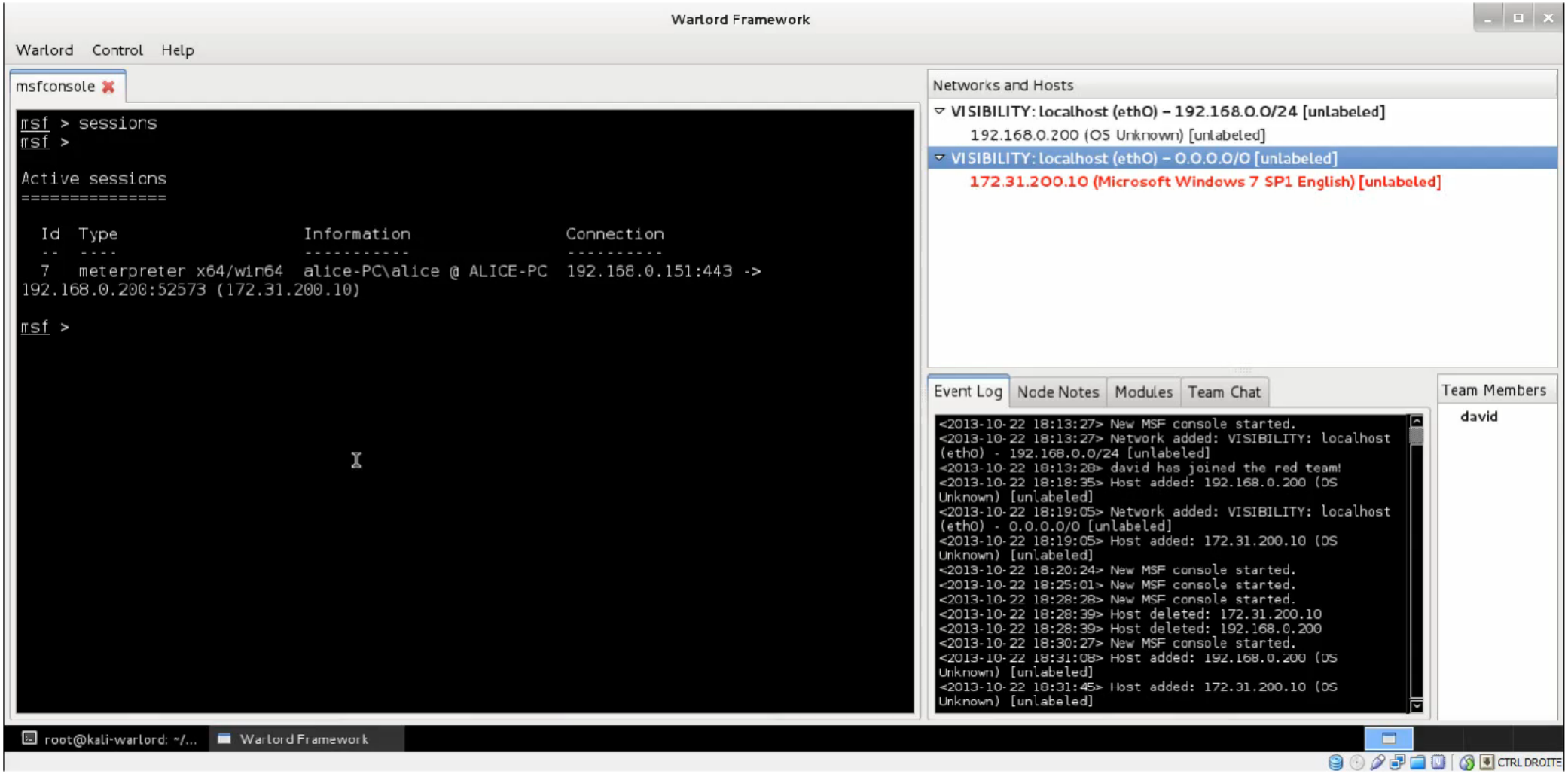
honeyrow

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