Cyber Careers - info from the field!

About me

academic stuff

- 2012 - BS Computer Science from ULL
- 2015 - MS Computer Science from UNO
  - Took pentesting w/ Roussev
  - ‘Dynamic Aspect Oriented Bytecode Instrumentation’ thesis
- 2019 - PhD from UNO
  - ‘Nugget: A language runtime for Digital Forensics and Incident Response’ thesis and other associated papers/conferences

About me

professional hacker at big corporations!

- 2012 - Begin work for Lockheed Martin (Lakefront campus)
  - software engineer (eww!!)
- 2014 - Transfer to corporate Red Team (hacking team)
  - work from home!!, classified work, CVEs
- 2018 - Grow to a senior lead position for Lockheed
- 2022 - Begin work for Thomson Reuters, as head Red Team analyst for the corporation

Cyber in Enterprise

Many domains within corporations

- Gather information from various sources
- Could be sourced from all over, classified (govt), open source, etc.

Intelligence

Vulnerability Management

- Continuously run scanners across the enterprise for unpatched services, open ports, etc
- Servers and endpoints
- Could easily be 100,000 devices in an enterprise

Security Operations Center (SOC)

- Continuously review data from endpoint detection and response (EDR) alerts
- If the alert looks suspicious, flag for investigation and/or incident response measures

Incident Response (CIRT)

- Investigate computer/server for malicious behavior using forensic techniques
- Isolate compromised machines

Red Team

- Emulate the adversary – attack your own enterprise!
- Build reports highlighting gaps in security
- Anything the bad guys do, you get to do
  - Physical testing, wireless, write ransomware, and more :)

Blue Team

- Catch the Red Team by building alerts
- Help mitigate any problems found by Red Team

All functions are often performed in-house, but can be from contractors

Skills / Knowledge foundations

Wide domain of cyber requires range of skills

Reporting and communication

- Human & technical
- Powerpoint
- Automated generation

Coding

- SQL knowledge for example lends itself to Splunk queries
- Python lets you quickly build scripts for various tasks

Networking

- Deep understanding of TCP/IP, HTTP

Storage

- FAT vs NTFS etc

Cloud

- AWS / Azure etc
- Platforms as a service (e.g., remote desktop)

Technologies

- Firewalls
- AV & EDR
- Splunk :)

It's critically important to be able to analyze data and communicate summaries, no matter the 'specialty' you end up pursuing

Common Security Products

Things you're likely to run into

Anti Virus
- MS Defender
- McAfee

EDR
- FireEye
- CrowdStrike

Firewalls
- Palo Alto
- Cisco

Analytics (SIEM)
- Splunk

Red Team
- Cobalt Strike
- Metasploit

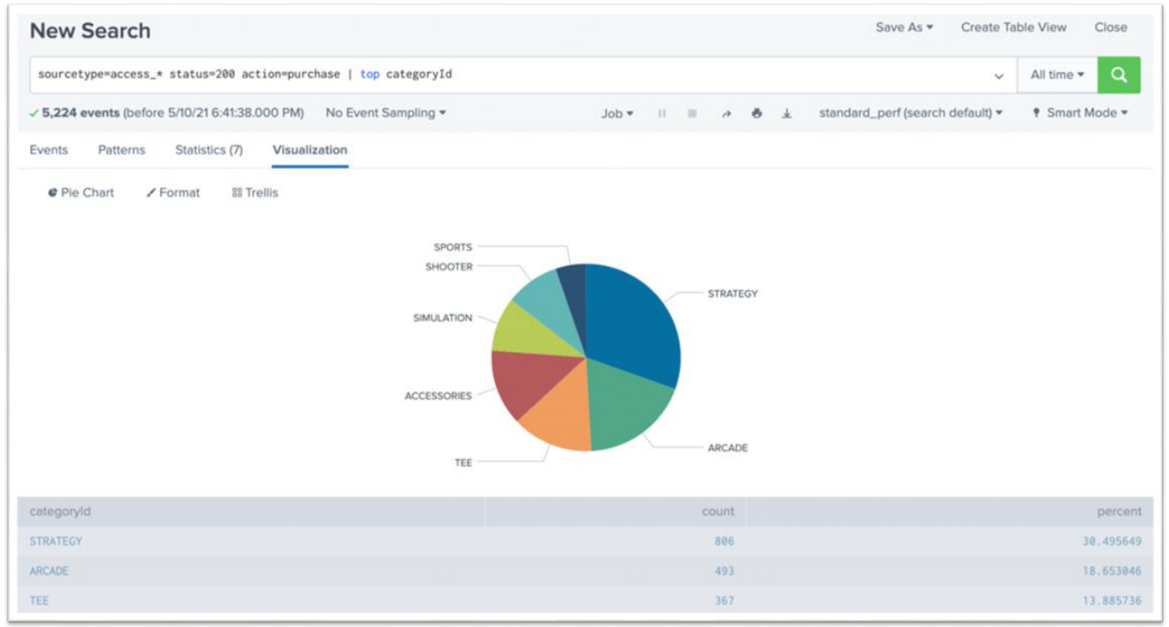
Intelligence
- Maltego
- RiskIQ

Many cross-pollinate across 'domains', and many have certificate paths

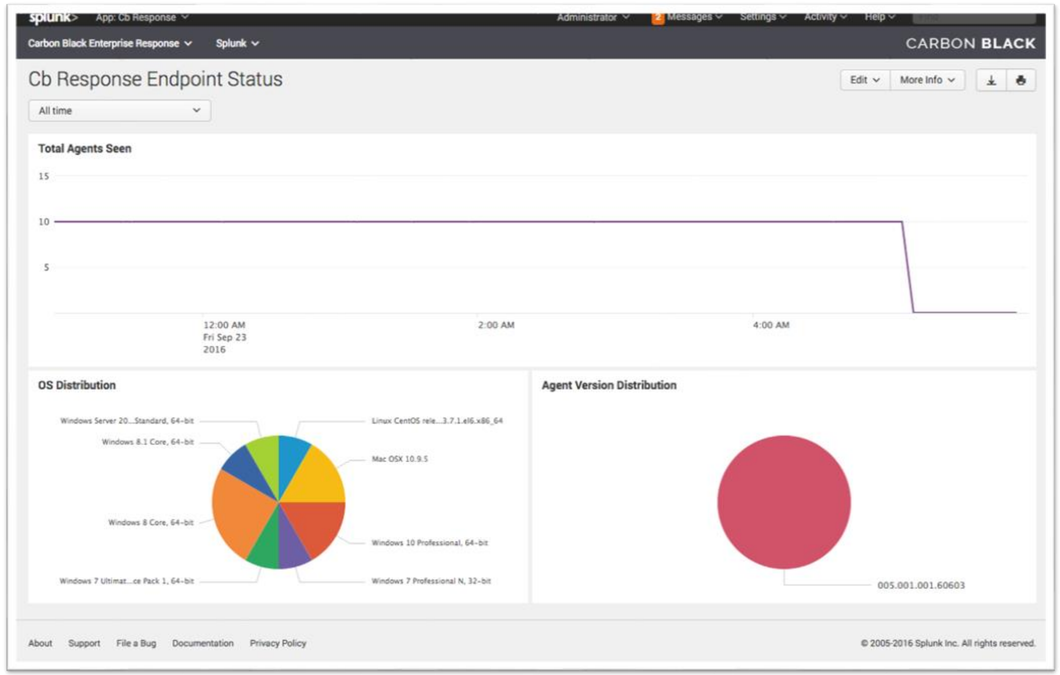
Let's talk Splunk

Like it or not, here it comes …

- Capture large amounts of JSON records
- Really can be anything
- Common for capturing all web requests to external facing servers
- Also can capture every time you execute a .exe on your Windows machine (across every computer in a corporation)



Splunk query for web logs ("who purchased what on 5/10/2021?")

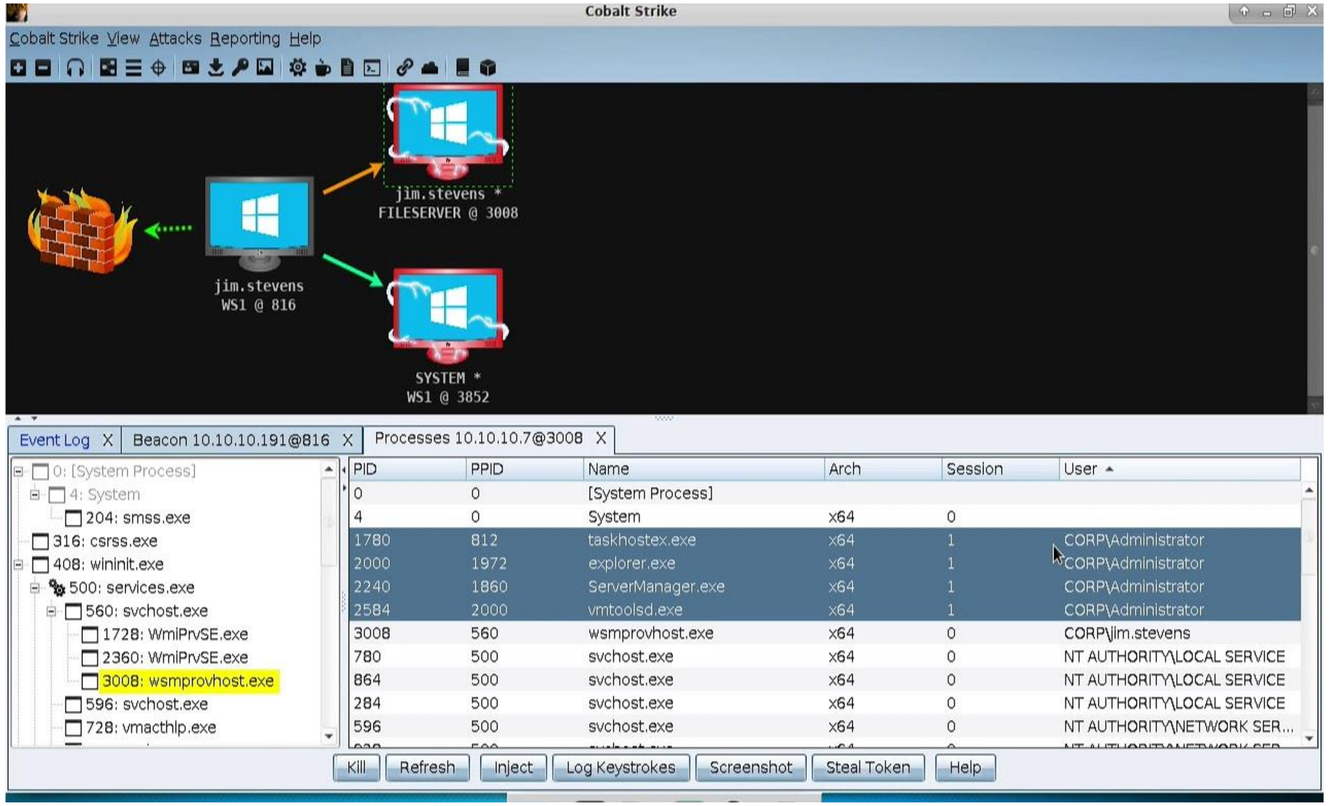


Splunk dashbaord for OS versions and what version of EDR agent is installed

Let's talk Cobalt Strike

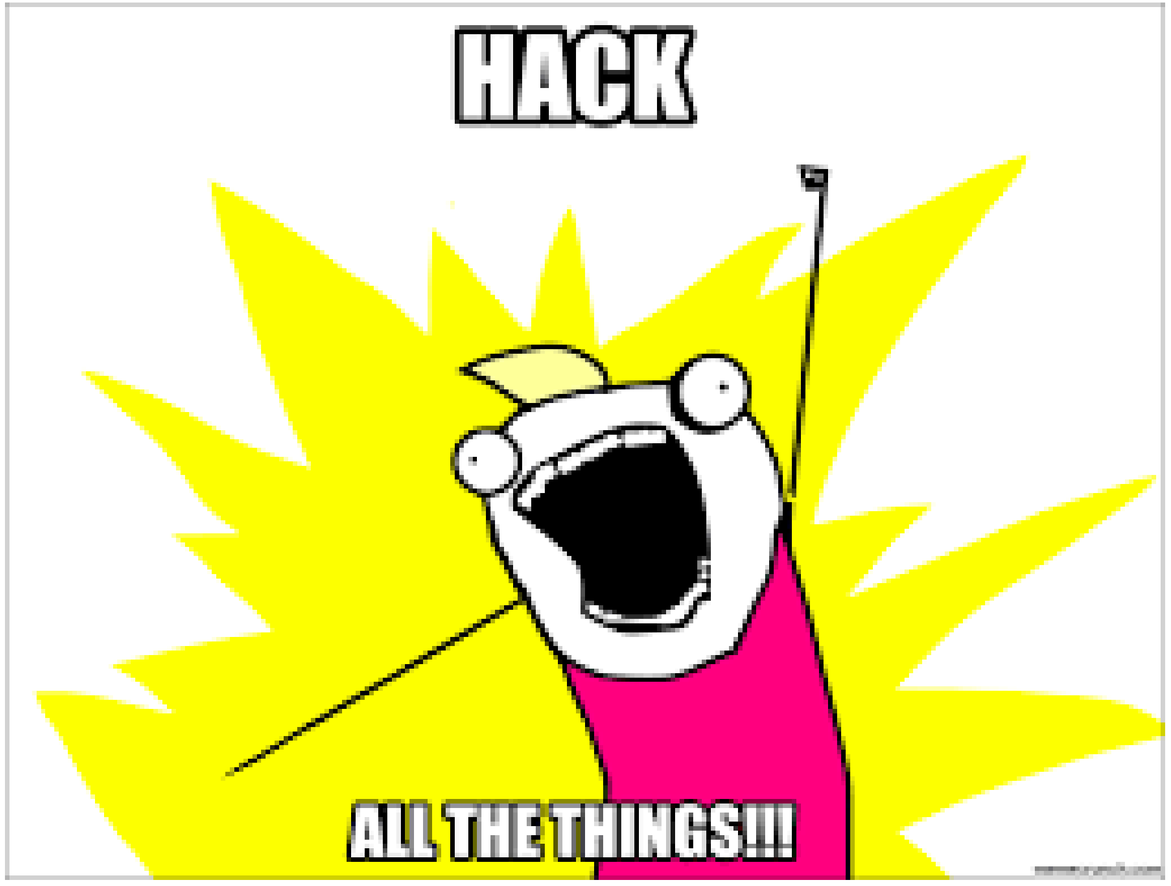
"Gold Standard" for Red Team (adversary emulation)

- DoD project that grew into commercial tool
- Cool graphical interface to show chains of compromised machines
- Useful to execute chained attacks
  - Packaged things like in-memory DLL injection, port scanning, powershell execution, etc.
- Fairly expensive; many open source alternatives



Cobalt Strike GUI showing a number of compromised hosts

Let's talk Red Teaming


HACK
ALL THE THINGS!!!


KEEP
CALM
AND
HACK ALL
THE THINGS

Penetration Testing / Red Teaming

what is it all about

- Find ‘cyber’ problems before real adversaries do
- Two main categories: Corporate Teams, Consulting Firms
  - **Corporate Teams** - work directly for the company, have more insight across organization and higher operational tempo
    - 2021 - Required for publicly traded companies
  - **Consulting Firms** - externals hired on a contract basis, typically evaluate for a few weeks and move on to another contract
- Combination of ‘White Box’ testing and ‘Black Box’ testing

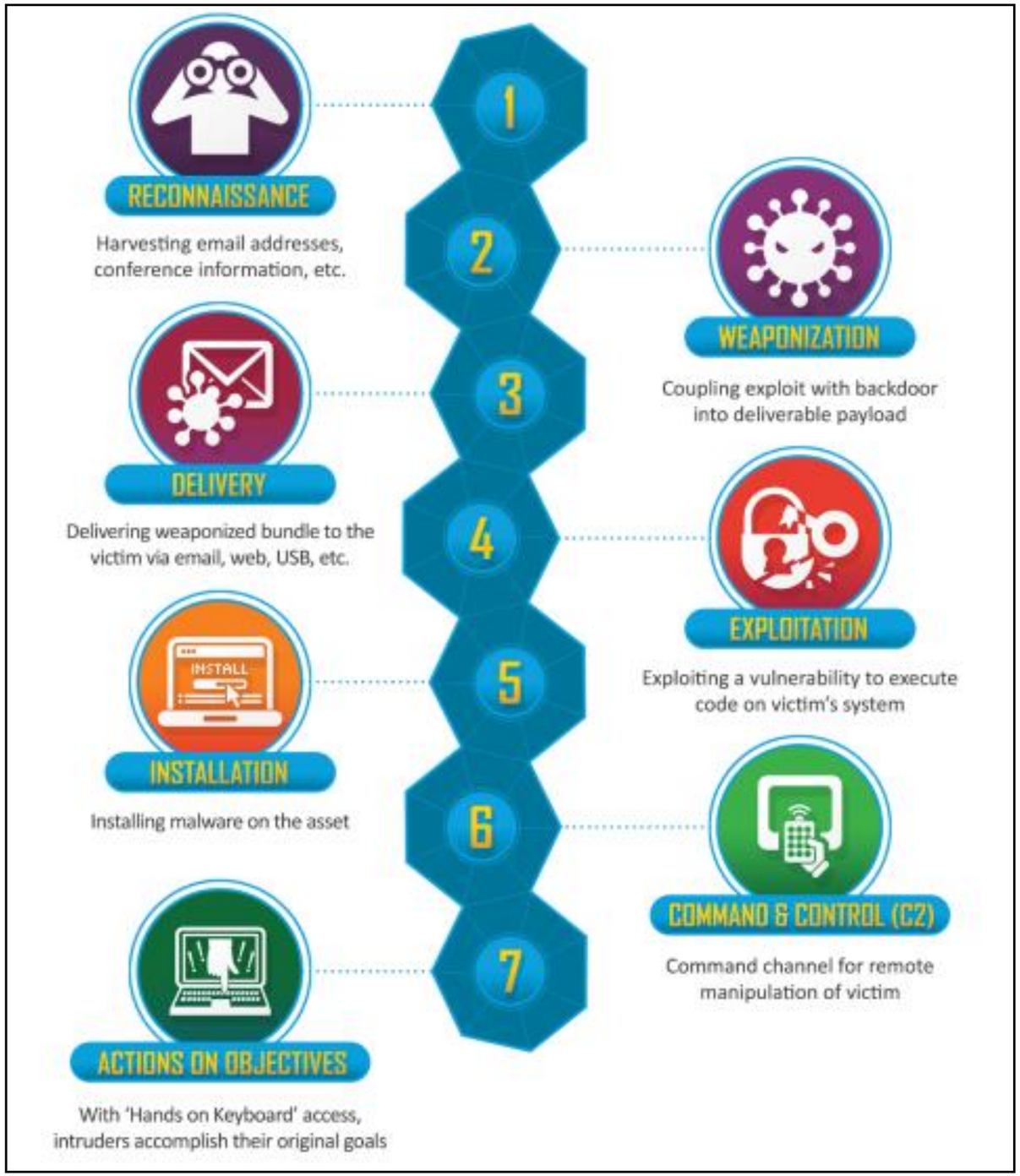
Mission Selection

how to decide what to hack?

- Can’t hack everything in one mission
  - Lockheed Martin for example has 120,000 employees and hundreds (thousands?) of different contracts
- Select bite-sized efforts
  - Examples: Slack implementation, Orion Capsule Dev Servers, or DNS exfiltration
- Influenced by intel teams
  - C-Suite executives, government advisories, or vendor advisories
- Or, ‘biggest revenue’ first

Cyber Kill Chain

Lockheed Martin



Example mission

‘Skype’

- Executive sees news article about our Skype, asks for a test
- Identify who legally owns the Skype servers, obtain permission
- Identify all related servers and services, schedule
- Begin execution loop
  - Recon, find VOIP port
  - Research VOIP service, find vulnerable version
  - Exploit; go back to recon
- Collect results, conduct briefing

Document EVERYTHING!

Example Documentation

yes, it's that important!

UNCLASSIFIED
Documentation and Reporting Tool (DART)

DART | Missions | Joint Submarine Program (Demo) (1701) Tests | Mission Stats | Logged in as redteam

Mission Test Cases for Joint Submarine Program (Demo)

+ Add New

	#	Test Objective	POC	Supporting Data	Test Result	Status
	4	(Dev) Port Scans	Dan	Manage Data (1)	Run	Approved / Final
	6	(Prod) Escalate Privileges in Production Enclave Finding	Roy	Add Data	Run	In work
	5	(Dev) Bypass Staging Environment Restrictions Finding	Chris	Manage Data (5)	Run	Ready for review
	7	(Prod) Web Server Denial of Service		Add Data	Not Run	Not started

* Drag & drop to reorder test cases

Copyright © 2016 Lockheed Martin Corporation | About v2.0.0

Documentation and Reporting Tool (DART)
UNCLASSIFIED

'DART' webapp generates DOCX →

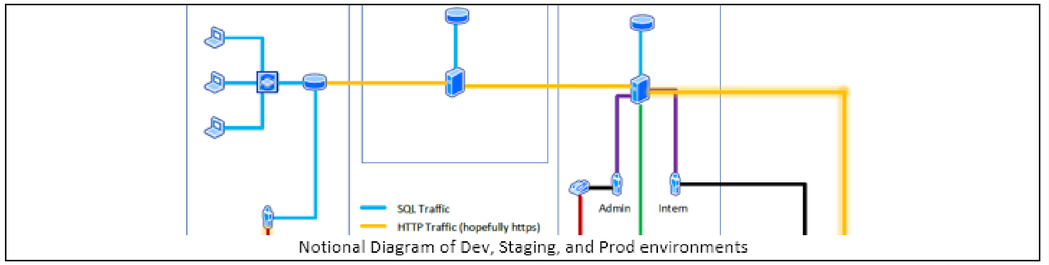
UNCLASSIFIED

Test #3	Bypass Staging Environment Restrictions
Attack Phase/Type:	Delivery - Elevation of Privilege
Assumptions:	Adversary has a presence in the Dev enclave
Description:	Attempt to push a malicious python script directly to the production server from the development enclave, bypassing the configuration management steps implemented in the staging enclave.
Findings:	- An unprivileged user can inject arbitrary code from the development enclave to the production enclave, bypassing the staging environment
Mitigations:	Implement a firewall to block direct network access from the development enclave to the production enclave.
Tools Used:	python
Command/Syntax:	python sendImplant.py
Target:	192.168.20.4 (Prod Web Server)
Attack Source:	192.168.20.4 (Prod Web Server)
Attack Date/Time:	Jan 16, 2017 @ 09:55 AM
Side Effects:	The production server generated an log entry indicating the script was not signed by the staging server, however the customer indicated this type of log entry is set off all the time due to configuration issues and is ignored if it's ever seen.
Details:	The malicious script was successfully transmitted to the production server without being reviewed in the staging environment. This allows for a C2 channel to be created between development and production environments.
Supporting Data:	- Makefile: Related makefile - rc-mgmt-es-ingest.txt: Example text file
Notes:	

UNCLASSIFIED

6.3.1 SCREENSHOTS / DIAGRAMS

UNCLASSIFIED



Notional Diagram of Dev, Staging, and Prod environments

UNCLASSIFIED

https://github.com/lmco/dart

Day in the life

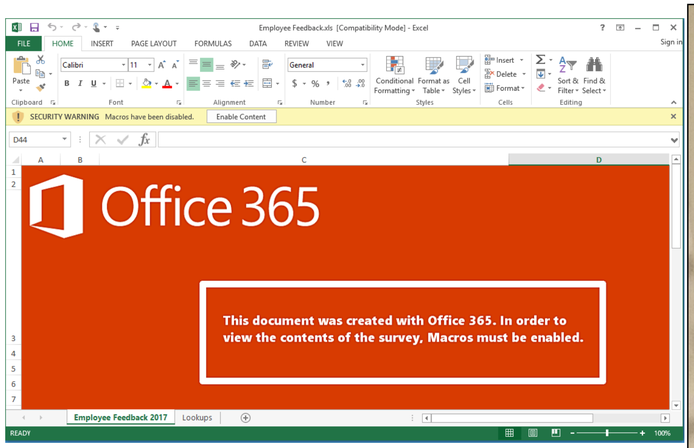
Red Teaming

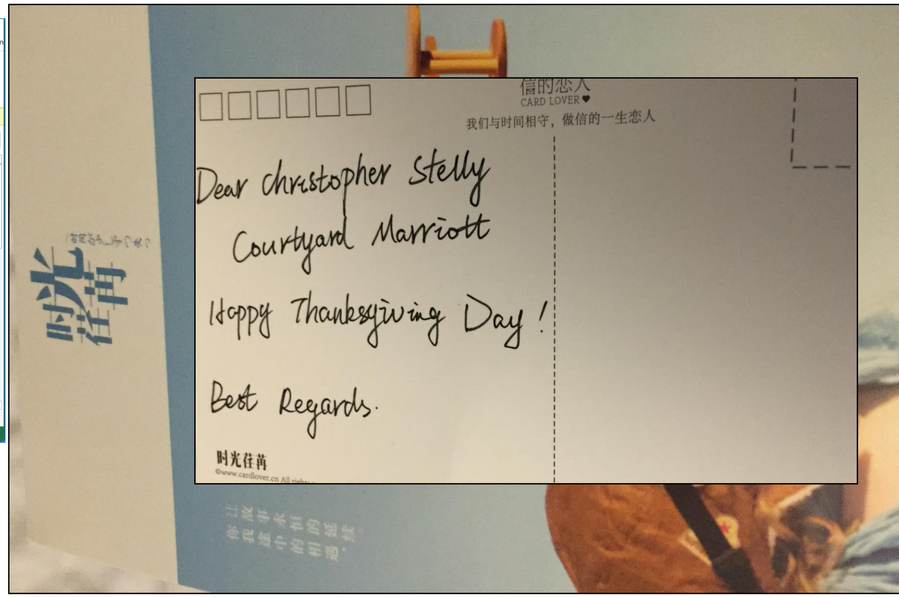
- Read intel reports [internal, twitter, whatever]
- Meet with team to discuss ongoing or upcoming missions, other organizational stuff
- Begin executing test cases for the day
  - **Continuously document results**
  - Goal: remote code execution!
- Spend time on building infrastructure
  - [external perimeter scanner, rotating IP scheme, new phishing tools, new domains, etc]
- Debriefs

Stories from the field

Red Teaming

- Japan physical pentest
- ‘Protect your backups’
- Phish with ‘employee salary’ xslx
- AV evasion
- Postcard
- Counter-intel





Resources

Getting Started

- Podcasts: SecurityNow, Sophos Naked Security
- Learning platforms:
  - **HackTheBox** (my username: Fiddler*…happy to help anytime)
  - TryHackMe (softer landing, includes how-to)
  - VulnHub
  - BurpSuite Labs
  - Bug Bounties (HackerOne)

* https://www.hackthebox.com/home/users/profile/318682

Useful Skills

Getting Started

- Networking skills!
  - wireshark is your best friend
- Linux and Windows command line: bash, sed, awk
- Scripting and coding: **python** and golang!
- Communication skills - how to handle people

Useful Tools

Getting Started

- Operating systems: Kali Linux, ParrotOS
- Reporting Tools: DART (open source from my old Lockheed Team), Vectr, Dradis
- Burpsuite
- Metasploit
- Linux-Exploit-Suggester.py

A word on certifications..

Getting Started

Common interview questions & tips

- Last time we talked, this seemed to pique interest
  - Describe what happens when you type ‘yahoo.com' into your search bar. (SSL/TLS)
  - Describe a typical pentesting engagement. (MOU - memo of understanding)
  - Explain symmetric and asymmetric encryption, including advantages to each.
  - Describe a script or tool you’ve written.
  - Why perform a pentest if you’ve got a vulnerability scanning team?
- Certifications: CEH (‘beginner’), OSCP (‘standard’)

Vulnlab

Burpsuite Free Labs

- Burpsuite: https://portswigger.net/burp/communitydownload
- Burpsuite Labs: https://portswigger.net/web-security/all-labs
- Our exercise today: https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-retrieve-files

Vulnlab

TryHackMe

- https://tryhackme.com/room/alfred

Documenting with DART!

- https://github.com/lmco/dart

  (setup)

Home Lab

Recommendations

- Server Virtualization: ProxMox Virtual Environment hypervisor
  - Hosts all OS types
- Setup a Windows domain (guide link)
  - Official Windows ISO downloads: https://www.microsoft.com/en-us/software-download/windows10
- Ubuntu, RedHat server(s)
- Kali attacking machine (taking snapshots often)

APT talk

What are the bad guys using?

- LAPSU$ gang - nVidia, Microsoft, Okta, Samsung hacks in 2022
  - Cookie stealing for initial access for SSO applications
  - Compromised email accounts to helpdesk systems to get into corporate VPNs
  - RDP for lateral movement - built in tools!
- Cobalt Strike, legitimate tool - awkward!
  - Leaked online - be careful if you seek it out