Red Teaming Workshop

Furkan ÖZER

Eylül 2023

Hakkımda

- Yıldız Teknik Üniversitesi – Bilgisayar Mühendisliği – 2018
- Sızma Testi Uzmanı – 2016
- Forestall – Kurucu Ortak – 2020
- LockedShields – Yeşil Takım Üyesi - 2019
- CS RANGER, OSCP, OSCE, CRTP, AWS CSAA
- frknozr.github.io / forestall.io/blog
- Twitter/Github/Gitlab - frknozr
- Borabay, Invoke-Ulubat, Kangal

Ajanda

- Active Directory Temelleri
  - Mantıksal Birimler ve Obje Türleri
  - Yetkili ve Yönetici (Admin) Objeler
  - Access Control Entry ve Access Control List Yapıları
  - Hash Türleri
  - Kimlik Doğrulama Protokolleri
    - Kerberos
      - Protokol Temelleri
      - Double Hop Sorunu
      - Unconstrained Delegation
      - Constrained Delegation
      - Constrained Delegation – Protocol Transition
      - Resource Based Constrained Delegation
    - NTLM
      - Protokol Temelleri
  - Trust Yapıları

- Bilgi Toplama
  - Powershell ile Bilgi Toplama
  - WinNT ile Lokal Bilgi Toplama
  - GPO ile Lokal Bilgi Toplama
  - LDAP ile Bilgi Toplama
    - ADExplorer
    - BloodHound

- Yatayda Yayılma / Yetki Yükseltme Yöntemleri
  - TTP 0x0 – Rogue Machine Account
  - TTP 0x1 – LLMNR & NBT-NS Poisoning
  - TTP 0x2 – Coerced Authentication
  - TTP 0x3 – NTLM Relay
  - TTP 0x4 – Internal Monologue
  - TTP 0x5 – AS-REPRoasting
  - TTP 0x6 – Kerberoasting

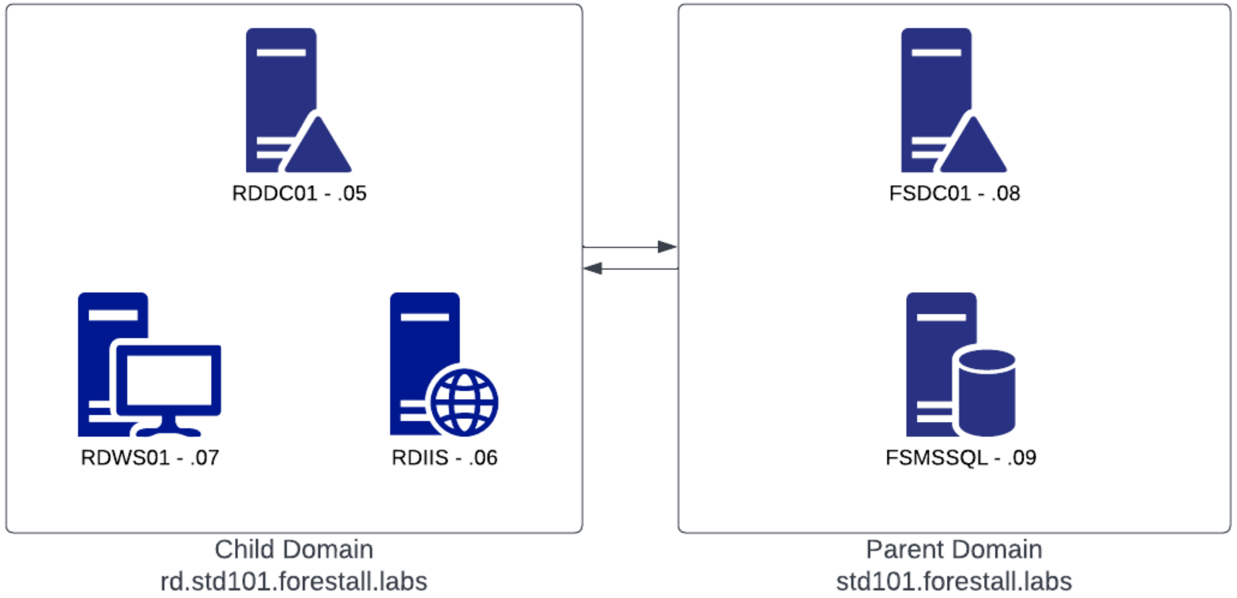
Ajanda

- Yatayda Yayılma / Yetki Yükseltme Yöntemleri
  - TTP 0x7 – GPP/GPO Exploitation
  - TTP 0x8 – ACL Exploitation
  - TTP 0x9 – S4U2Self Exploitation
  - TTP 0x10 – Pass the Hash
  - TTP 0x11 – Over Pass the Hash
  - TTP 0x12 – Pass the Ticket

- Kalıcılık Sağlama
  - TTP 0x13 – DCSync
  - TTP 0x14 – DCShadow
  - TTP 0x15 – ACL Backdoor
  - TTP 0x16 – AdminSDHolder Backdoor
  - TTP 0x17 – Skeleton Key

- Domainler/Forestlar Arası Geçiş
  - TTP 0x18 – Golden Ticket w/ SIDHistory
  - TTP 0x19 – Forged Trust Tickets
  - TTP 0x20 – Unconstrained Delegation w/ Spoolsvc
  - TTP 0x21 – PrivExchange

Lab Ortamı



Sunucu	IP Adresi
RDDC01	172.31.<NO>.5
RDIIS	172.31.<NO>.6
RDWS01	172.31.<NO>.7
FSDC01	172.31.<NO>.8
FSMSSQL	172.31.<NO>.9
Kali	172.31.<NO>.10

https://github.com/forestallio/ActiveDirectoryRedTeaming

HOW TO EVALUATE ENTERPRISE SECURITY

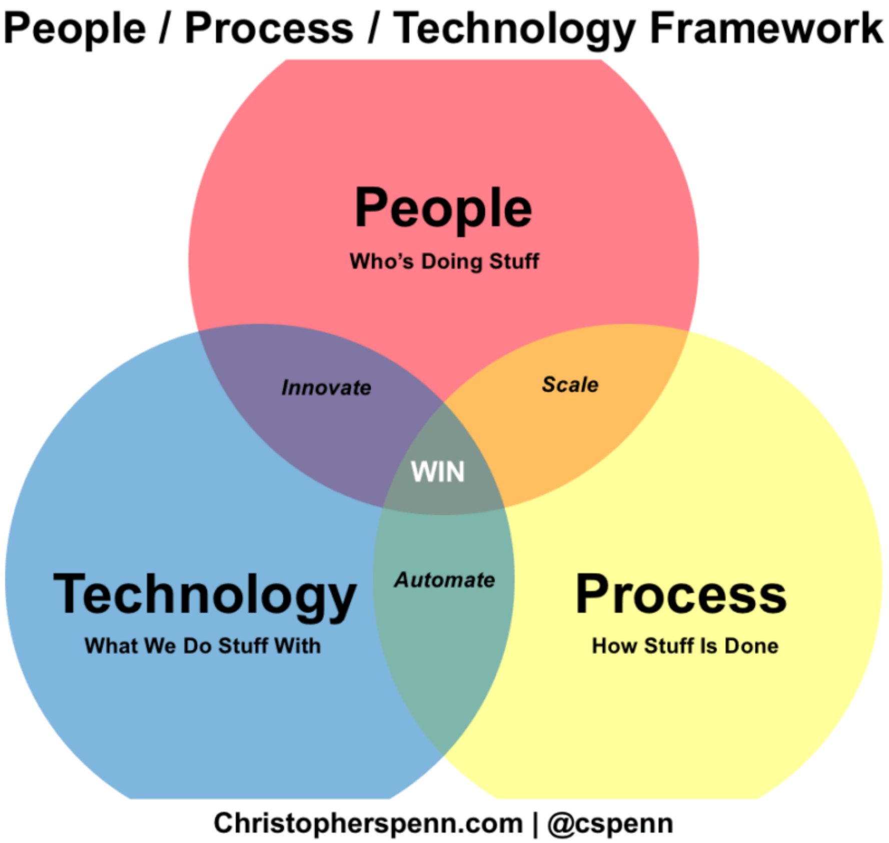
VULNERABILITY ASSESSMENT

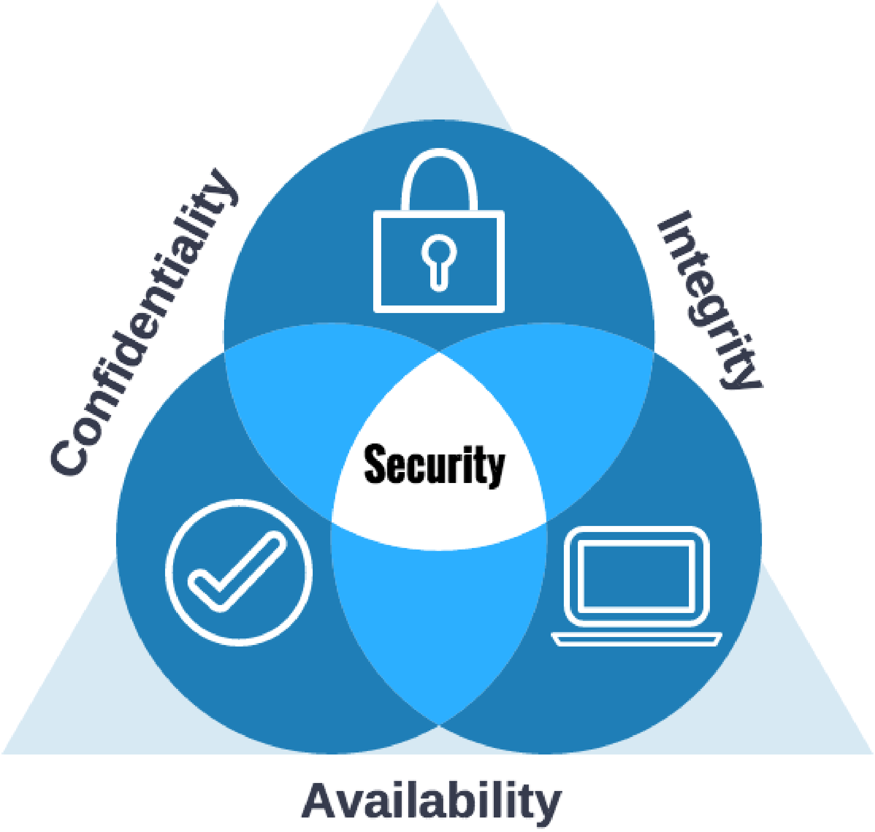
PENETRATION TESTING

RED TEAM ASSESSMENT

BREACH & ATTACK SIMULATION

Enterprise Security Pillars





Red Teaming

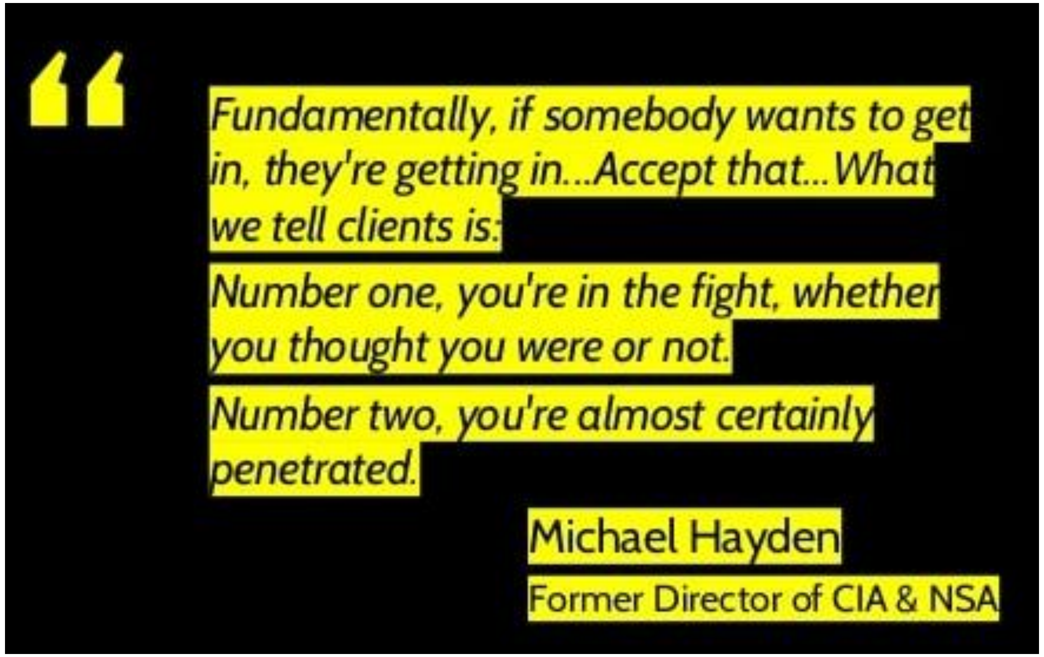
- Adversary Perspective – OPSEC Matters
- Objective Based Simulation
- Custom TTP's – Needs TI
- Also a training – Hacking to get caught
- What if?
- Types
    - Table top exercises
    - Physical attacks
    - Phishing
    - War-game exercises
    - Full scale cyber operation
    - Assume Breach
    - Adversary Simulation

We don't rise to the level of our expectations,
We fall to the level of our training.

Archilochus

Red Teaming

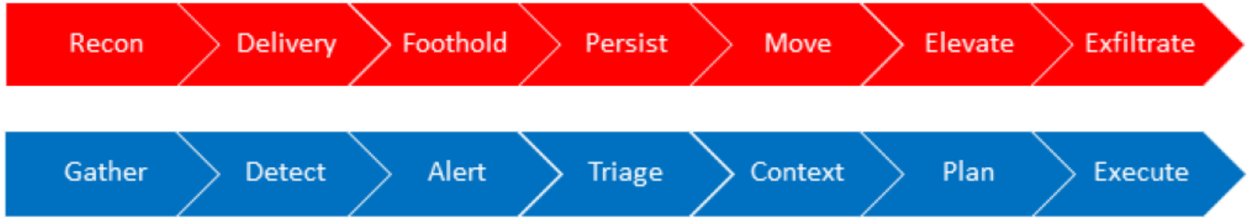
- Technology
  - Detection Products (AV, EDR, XDR, SIEM)
  - Product Policies & Rules
- People
  - Blue team maturity & tech skills
  - Blue team communication
  - Awarenesss
- Process
  - Crysis management
  - Detection processes
- Metrics
  - Mean Time to Compromise (MTTC)
  - Mean Time to Pwnage (MTTP)
  - Mean Time to Detection (MTTD)
  - Mean Time to Recovery (MTTR)



> "Fundamentally, if somebody wants to get in, they're getting in...Accept that...What we tell clients is:
>
> Number one, you're in the fight, whether you thought you were or not.
>
> Number two, you're almost certainly penetrated.

Michael Hayden

Former Director of CIA & NSA



Threat Modeling

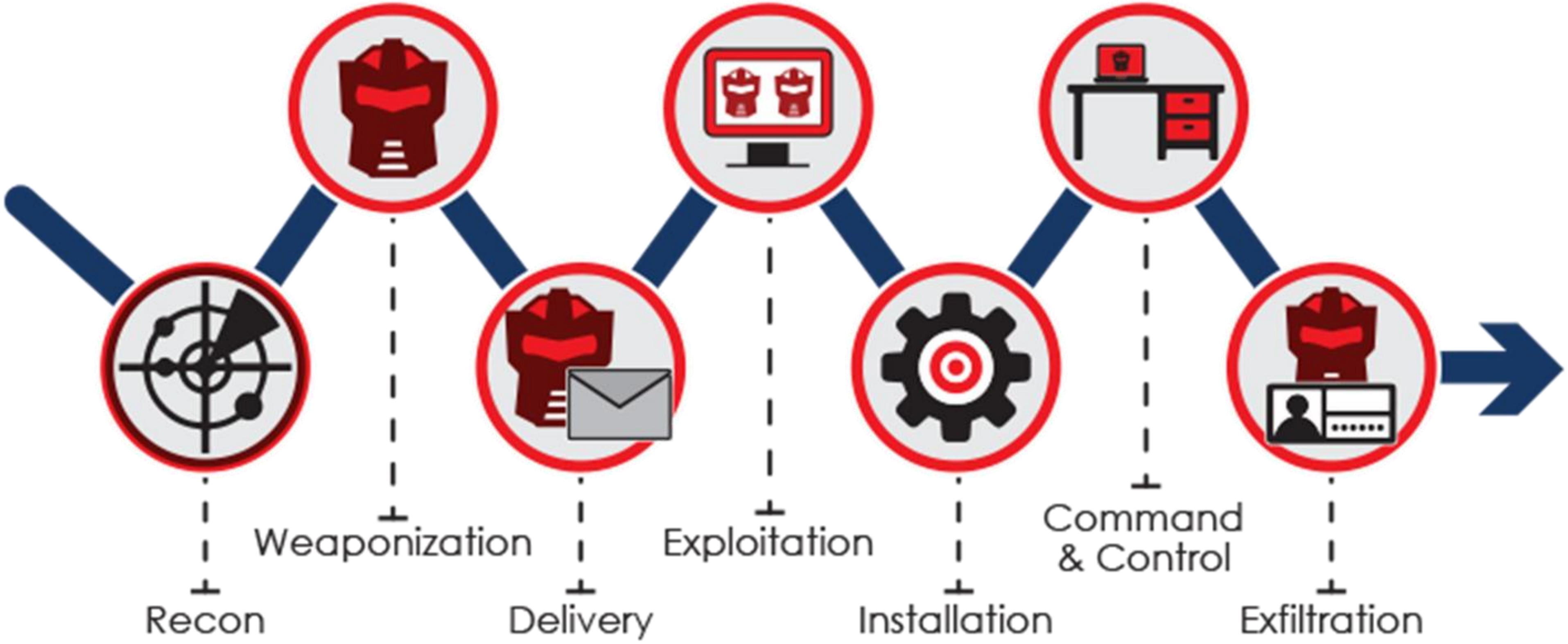
Red Teaming

- WHO is targeting us?
  - APT Groups
  - Competitors
  - Hacktivists
- WHAT is their motivation?
  - Corporate Espionage
  - PII & CC Exfiltration
  - Disrupting availability
  - Defacement & Propaganda
- WHICH areas do we need to strengthen?
  - Employee security awareness
  - Preventing data exfiltration
  - DoS/DDoS attacks
  - Integrity Checks & App Security

- DEFINE Red Team goals.
  - Exfiltrate PII data.
  - Find our next acquisition move.
  - Find our next target market country.
  - Compromise our CEO's e-mail account.
  - Infiltrate our CEO's office.
  - Deface our main page.
- CREATE suitable TTP's
  - E-mail with malicious word document
  - Custom POST Flood script
  - RFID Card cloning
  - Custom C2
  - Custom malware based on recon

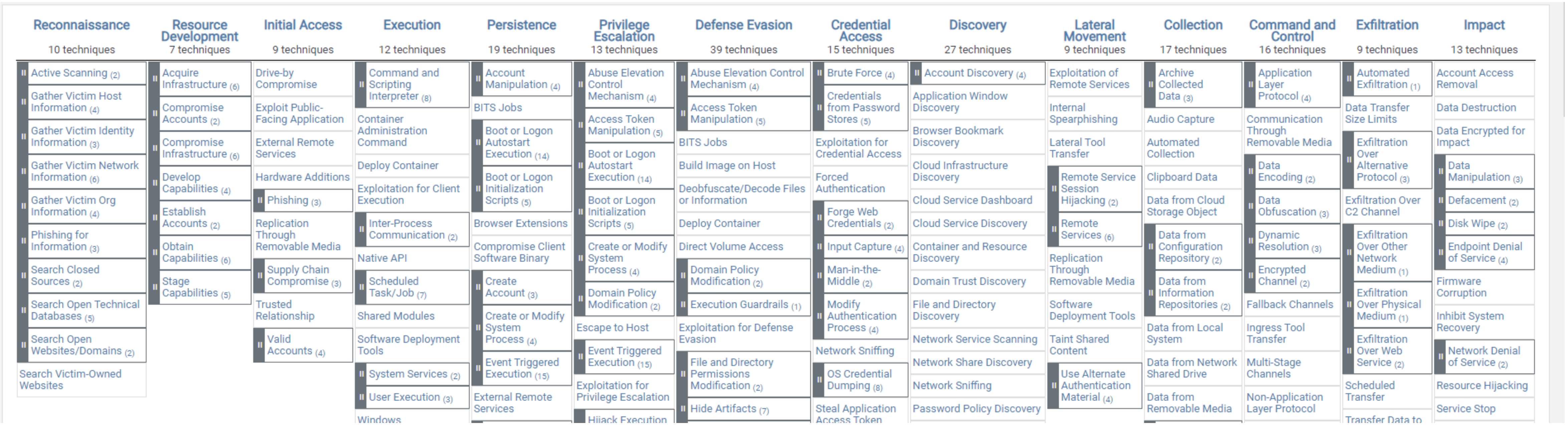
Cyber Kill Chain

Red Teaming



MITRE ATT&CK Framework

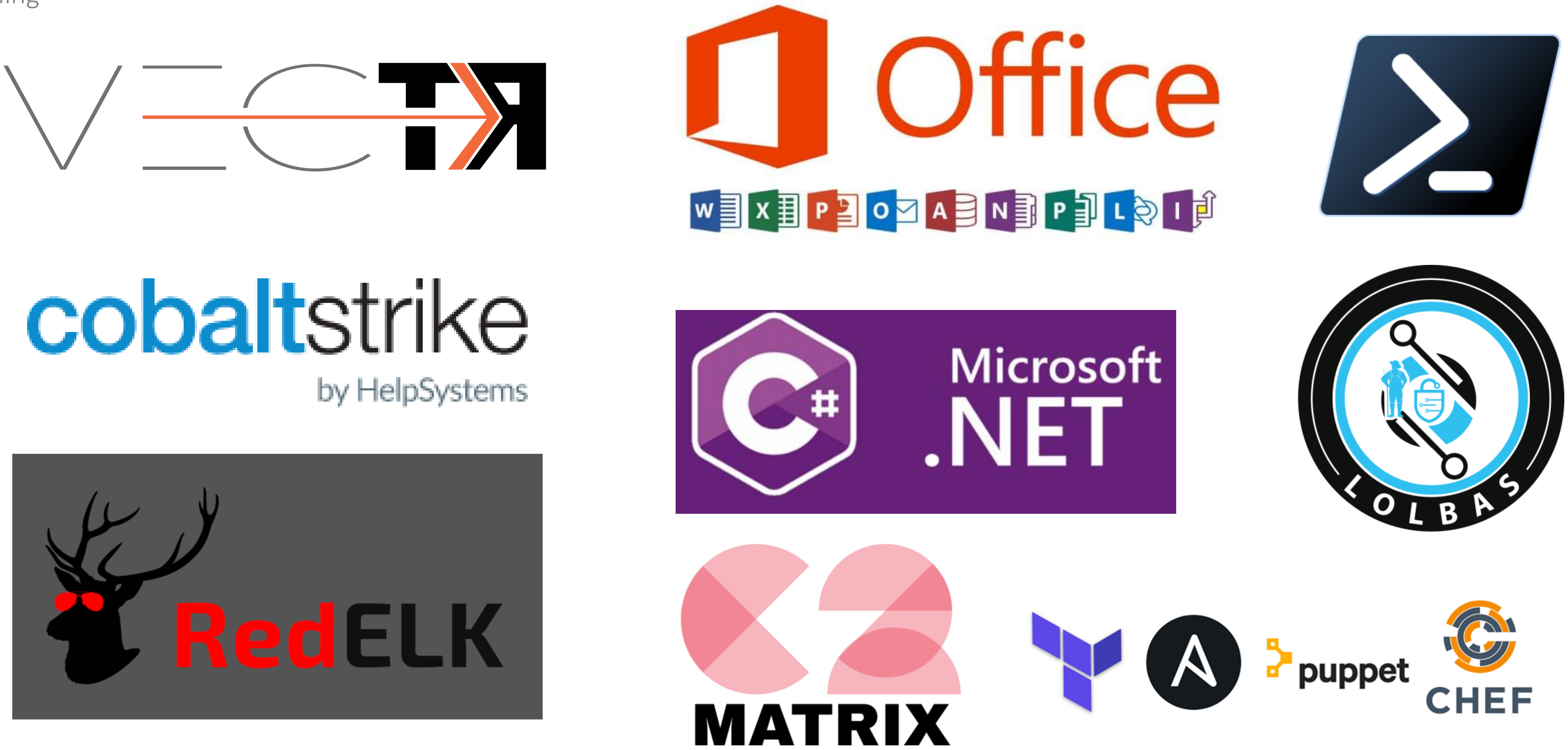
Red Teaming



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution	Exploitation for Defense Evasion	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)			File and Directory Permissions Modification (2)	Steal Application Access Token	Network Share Discovery					Resource Hijacking
			Windows			Hide Artifacts (7)		Network Sniffing					Service Stop
								Password Policy Discovery					

Tools

Red Teaming



Command & Control

Red Teaming

Key Points

Red Teaming

- Learn to develop custom tools / malwares
- Read APT and related reports for new TTP’s
- Learn devops for automated Red Team infra
- Log and document every steps of operation
- Learn logging & detection techniques for bypassing them
- OPSEC is crucial for Red Team ops
- House Cleaning

Comparison

Summary

	Vulnerability Assessment	Penetration Testing	Red Teaming
Scope	Wide & Superficial	Narrow & Deep	Narrow & Deep
Budget	Cheap	Medium	Expensive
Frequency	High	Medium – Low (Annualy)	Low
Tech Skills Required	Low	High	Ultimate
F/P Rate	High	Low - None	None
Type	Automated	Partially Automated	Manual
Actionability	Slow	Fast	Fast
Target	Technology	Technology & Process	Technology & Process & People
Intrusion	Low - None	Medium	High
Recommendation	Insufficient	Efficient	Efficient
Target Function	Prevention	Prevention	Detection

Covert Attack Infrastructure

Red Teaming

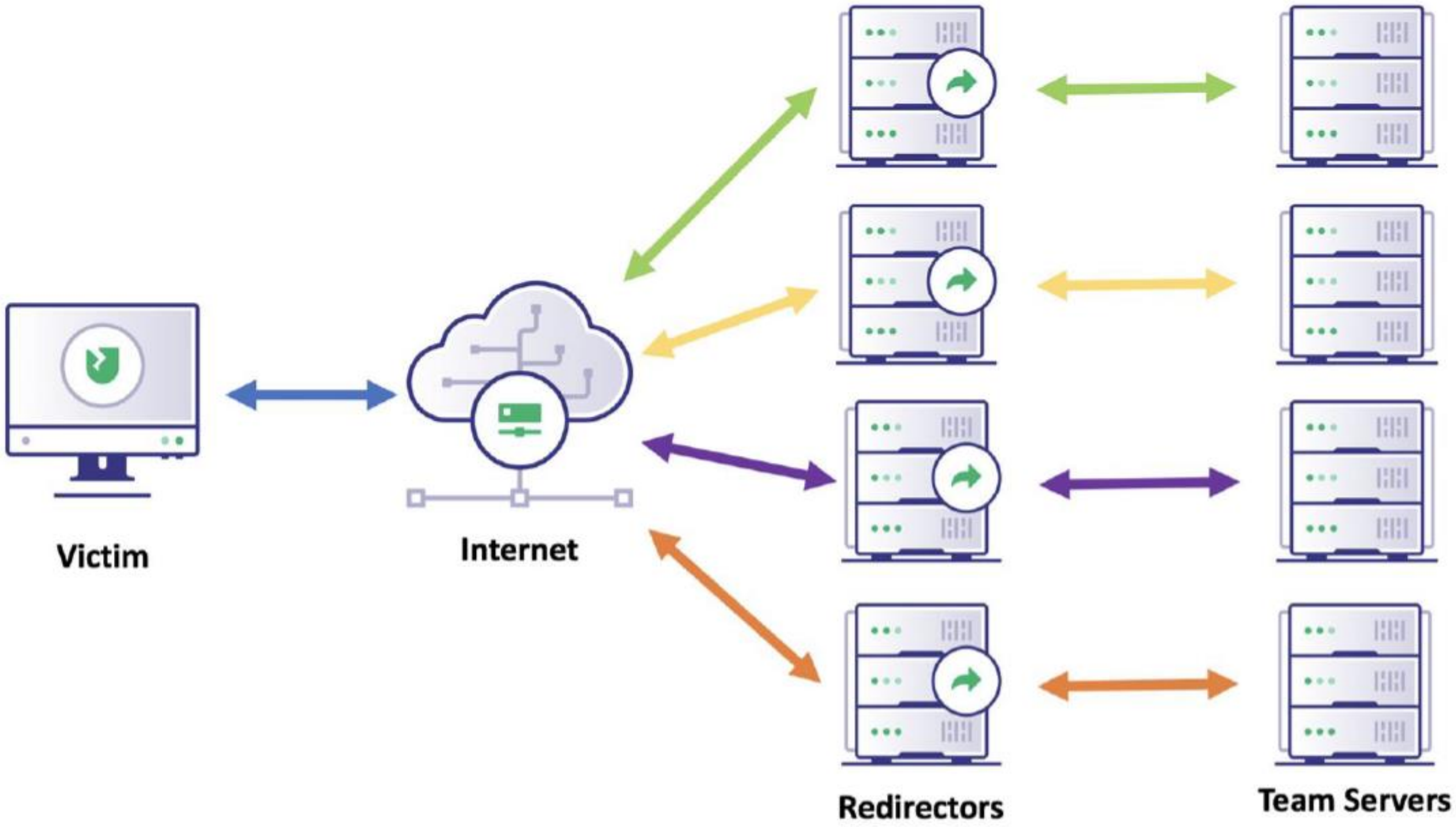
- Use Domain Fronting with redirectors
  - **Pass through**
  - **Smart Redirection**

- Use HTTPS always

- Automate deployment with Infra as Code

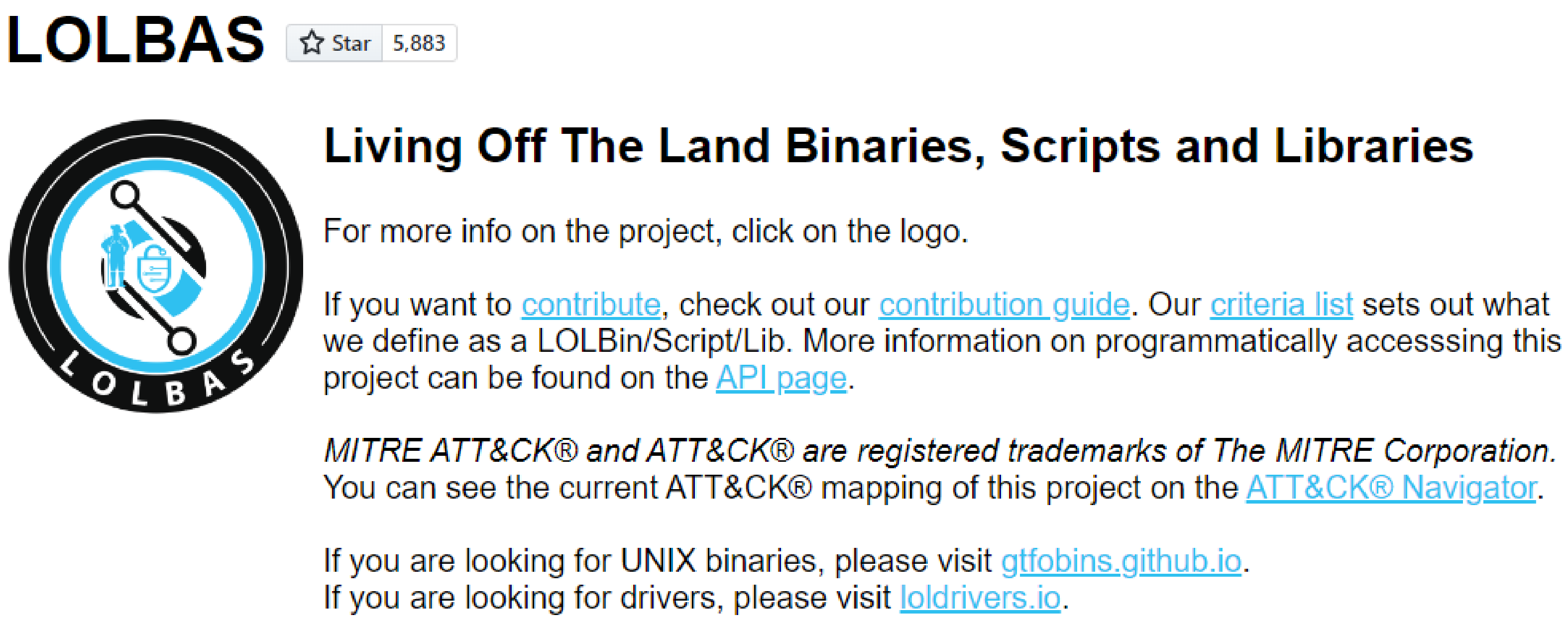
- Use expired categorized domains

- Monitor the infra



LOLBAS

Red Teaming



LOLBAS

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib. More information on programmatically accesssing this project can be found on the API page.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.
You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.
If you are looking for drivers, please visit loldrivers.io.