Navigating the Network: Active Directory Attacks and OPSEC Strategies

ROOTCON18 Red Teaming Village

About Me

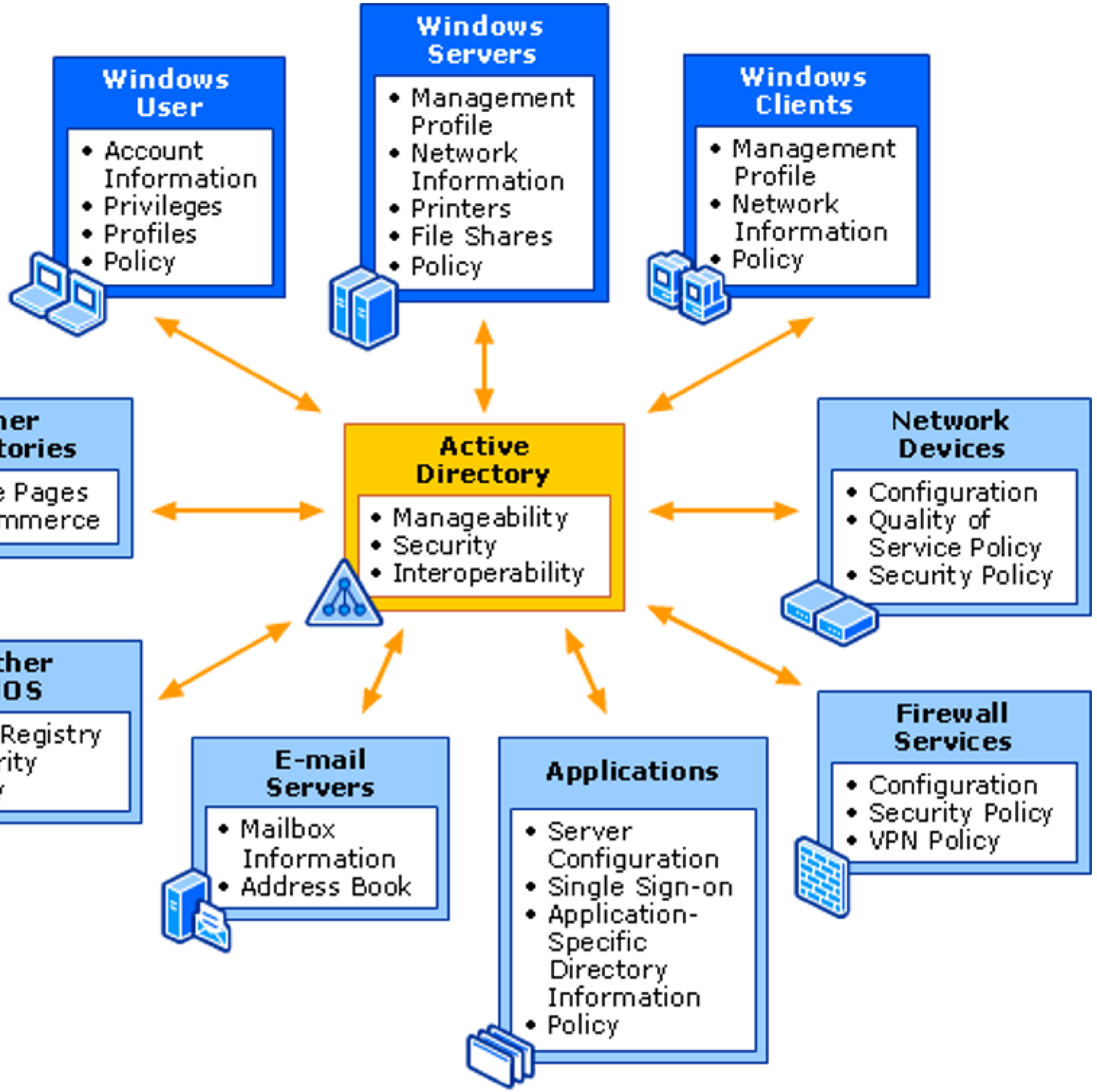
- Offsec Manager @ Red Rock IT Security Inc.
- SANS Instructor (SEC560)
- MSISE Student @ SANS Technology Institute
- Master in Information Security @ DLSU Manila
- GSP, GX-PT, GX-IH, GMOB, GPEN, GCIH, CISSP, OSEP, OSCP etc.

OUTLINE

- What is Active Directory?
- What is Red Teaming?
- What is OPSEC?
- Active Directory Attack Cycle
- OPSEC Considerations

What is Active Directory?

- **Microsoft's proprietary directory service to manage Windows networks**
- **A database that stores information of users, groups, computers, group policies, etc. stored in a domain controller**
  - A server that helps manage the whole AD database.
  - Usernames and passwords are stored here.
- **Changes to the AD database are replicated to other domain controllers inside the domain**



Active Directory
- Manageability
- Security
- Interoperability

Windows User
- Account Information
- Privileges
- Profiles
- Policy

Windows Servers
- Management Profile
- Network Information
- Printers
- File Shares
- Policy

Windows Clients
- Management Profile
- Network Information
- Policy

Other Directories
- White Pages
- E-Commerce

Network Devices
- Configuration
- Quality of Service Policy
- Security Policy

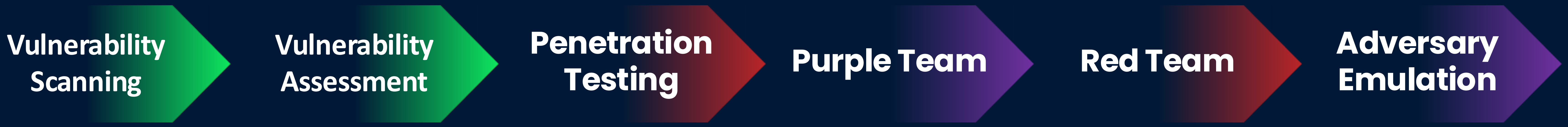
Other NOS
- User Registry
- Security
- Policy

E-mail Servers
- Mailbox Information
- Address Book

Applications
- Server Configuration
- Single Sign-on
- Application-Specific Directory Information
- Policy

Firewall Services
- Configuration
- Security Policy
- VPN Policy

Ethical Hacking Maturity Model



Vulnerability Scanning

Vulnerability Assessment

Penetration Testing

Purple Team

Red Team

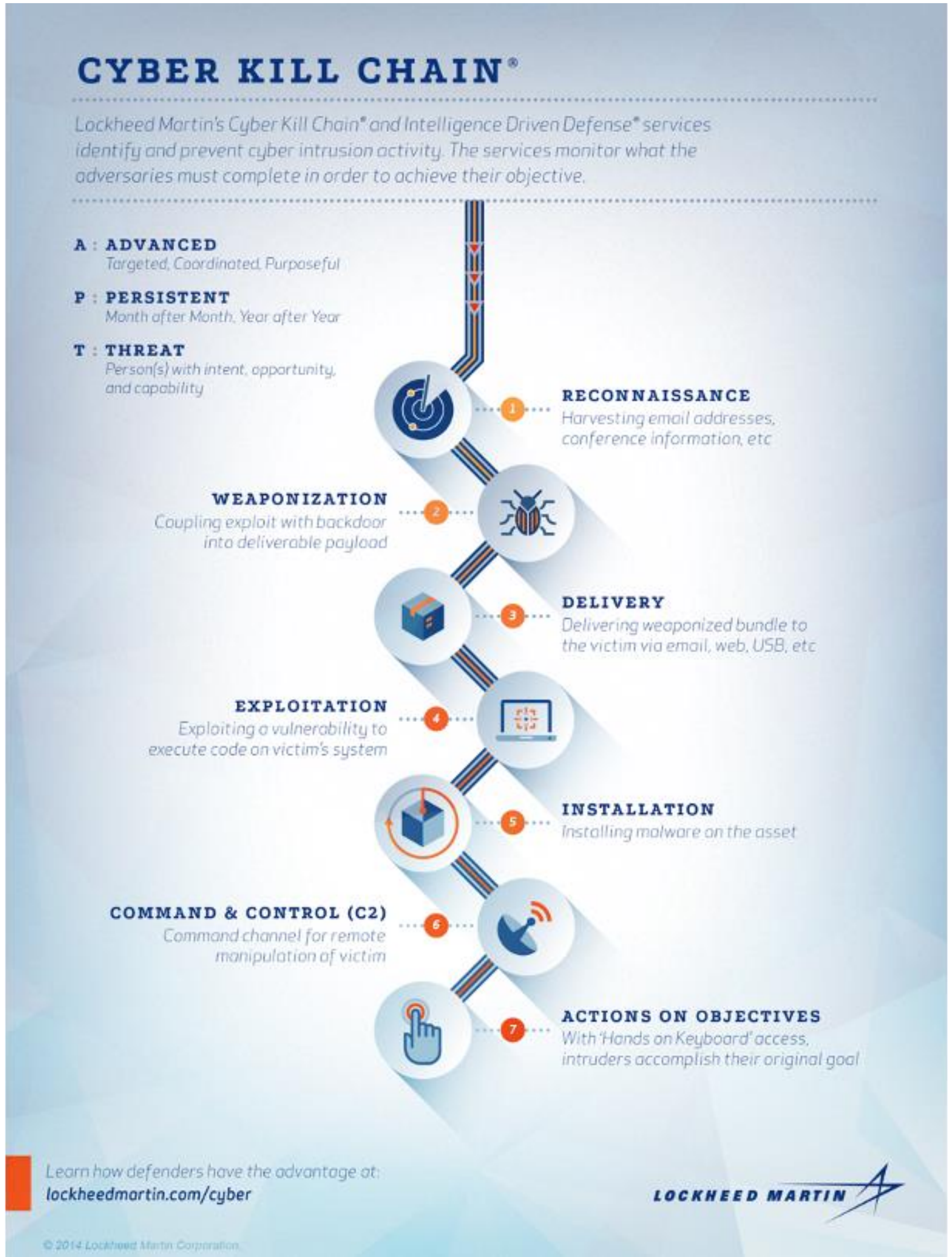
Adversary Emulation

What is Red Teaming?

> The practice of looking at a problem or situation from the perspective of an adversary.”
>
> - Red Team Journal

Why Red Team?

- **Identify and understand where the organization is currently at**
  - Are we really secure as we think we are?
- **Test people, process, technology**
  - Not focusing on vulnerabilities "CVEs"
- **Train and improve the blue team**
  - The blue team actively looks for and responds to malicious activity



CYBER KILL CHAIN®

Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

A : ADVANCED
Targeted, Coordinated, Purposeful

P : PERSISTENT
Month after Month, Year after Year

T : THREAT
Person(s) with intent, opportunity, and capability

1 **RECONNAISSANCE**
Harvesting email addresses, conference information, etc

2 **WEAPONIZATION**
Coupling exploit with backdoor into deliverable payload

3 **DELIVERY**
Delivering weaponized bundle to the victim via email, web, USB, etc

4 **EXPLOITATION**
Exploiting a vulnerability to execute code on victim's system

5 **INSTALLATION**
Installing malware on the asset

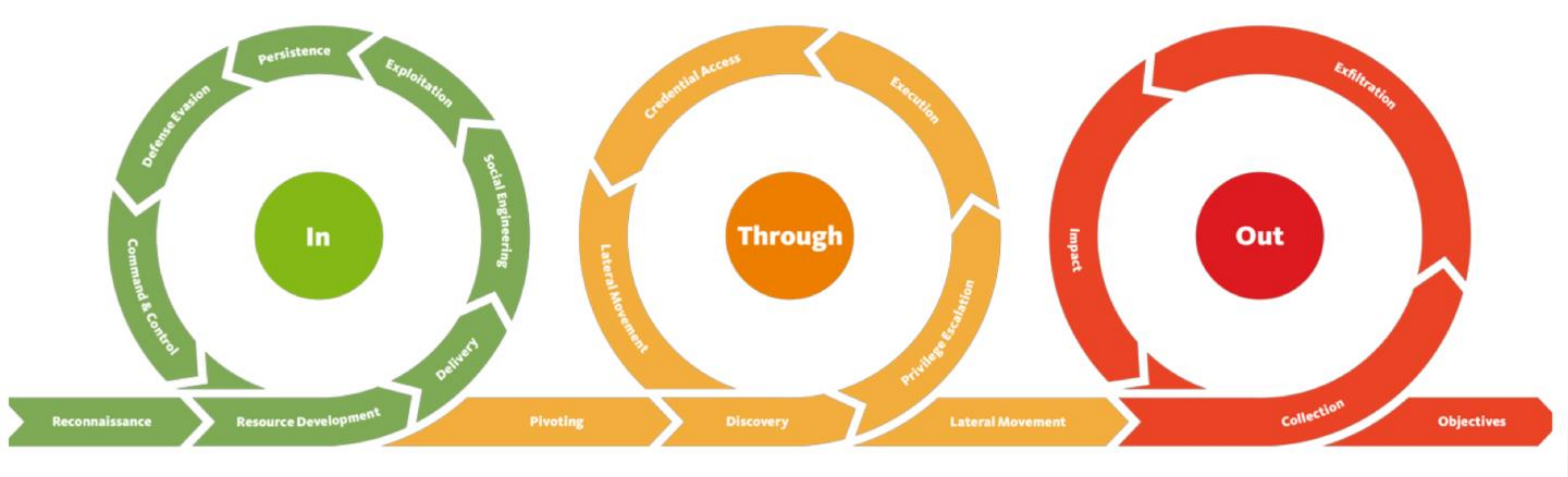
6 **COMMAND & CONTROL (C2)**
Command channel for remote manipulation of victim

7 **ACTIONS ON OBJECTIVES**
With 'Hands on Keyboard' access, intruders accomplish their original goal

Learn how defenders have the advantage at:
lockheedmartin.com/cyber

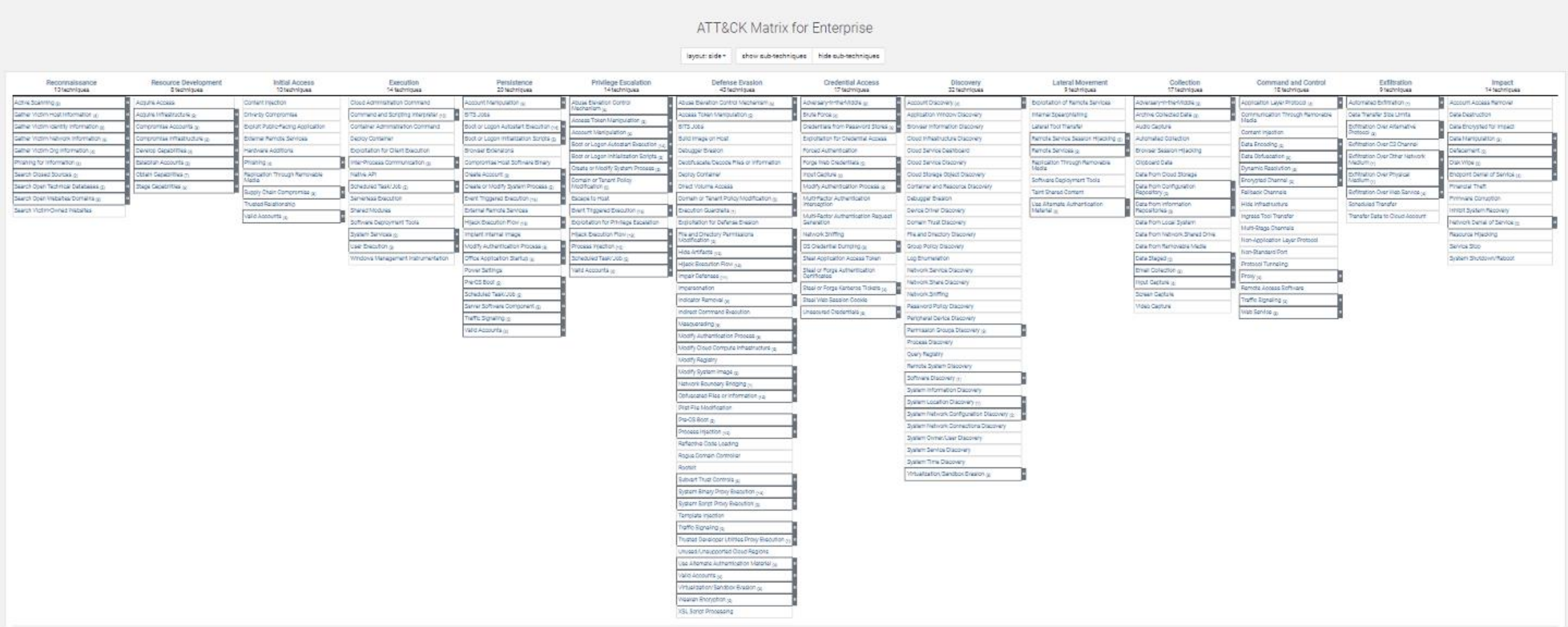
LOCKHEED MARTIN

Unified Kill Chain



https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

MITRE ATT&CK

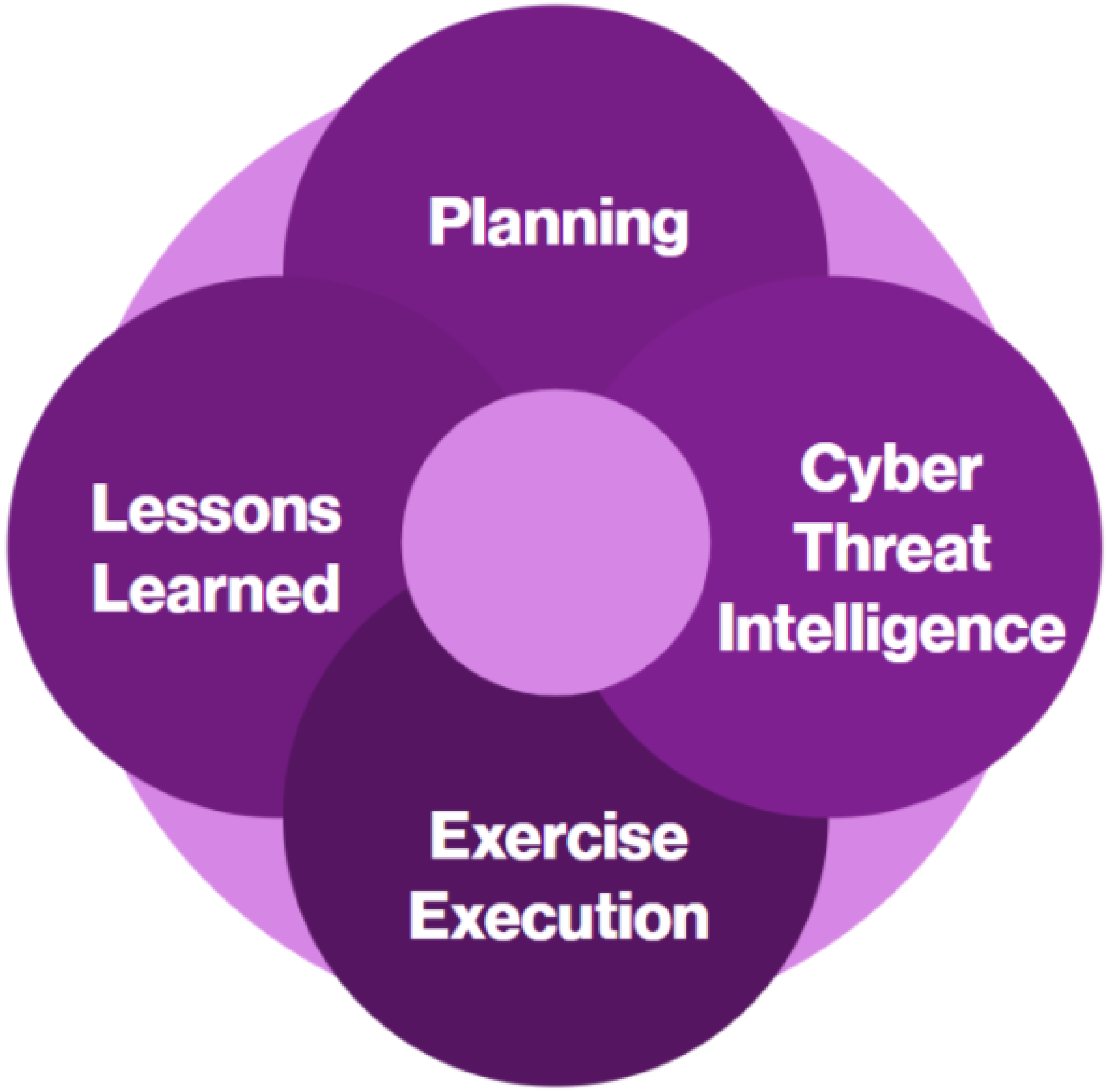


ATT&CK Matrix for Enterprise

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain or Tenant Policy Modification (2)
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)
			Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Exploitation for Defense Evasion
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)
			User Execution (3)	Modify Authentication Process (8)	Scheduled Task/Job (5)	Hide Artifacts (12)
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (12)
				Power Settings		Impair Defenses (11)
				Pre-OS Boot (5)		Impersonation
				Scheduled Task/Job (5)		Indicator Removal (9)
				Server Software Component (5)		Indirect Command Execution
				Traffic Signaling (2)		Masquerading (9)
				Valid Accounts (4)		Modify Authentication Process (8)
						Modify Cloud Compute Infrastructure (5)
						Modify Registry
						Modify System Image (2)
						Network Boundary Bridging (1)
						Obfuscated Files or Information (12)
						Plist File Modification
						Pre-OS Boot (5)
						Process Injection (12)
						Reflective Code Loading
						Rogue Domain Controller
						Rootkit
						Subvert Trust Controls (6)
						System Binary Proxy Execution (14)
						System Script Proxy Execution (2)
						Template Injection
						Traffic Signaling (2)
						Trusted Developer Utilities Proxy Execution (1)
						Unused/Unsupported Cloud Regions
						Use Alternate Authentication Material (4)
						Valid Accounts (4)
						Virtualization/Sandbox Evasion (3)
						Weaken Encryption (2)
						XSL Script Processing

Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (5)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (2)
OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking
Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		Service Stop
Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Protocol Tunneling		System Shutdown/Reboot
Steal or Forge Kerberos Tickets (4)	Network Service Discovery		Input Capture (4)	Proxy (4)		
Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Software		
Unsecured Credentials (8)	Network Sniffing		Video Capture	Traffic Signaling (2)		
	Password Policy Discovery			Web Service (3)		
	Peripheral Device Discovery					
	Permission Groups Discovery (3)					
	Process Discovery					
	Query Registry					
	Remote System Discovery					
	Software Discovery (1)					
	System Information Discovery					
	System Location Discovery (1)					
	System Network Configuration Discovery (2)					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion (3)					

Purple Team Exercise Framework (PTEF)



https://github.com/scythe-io/purple-team-exercise-framework

Red Team

Definitions:

A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.

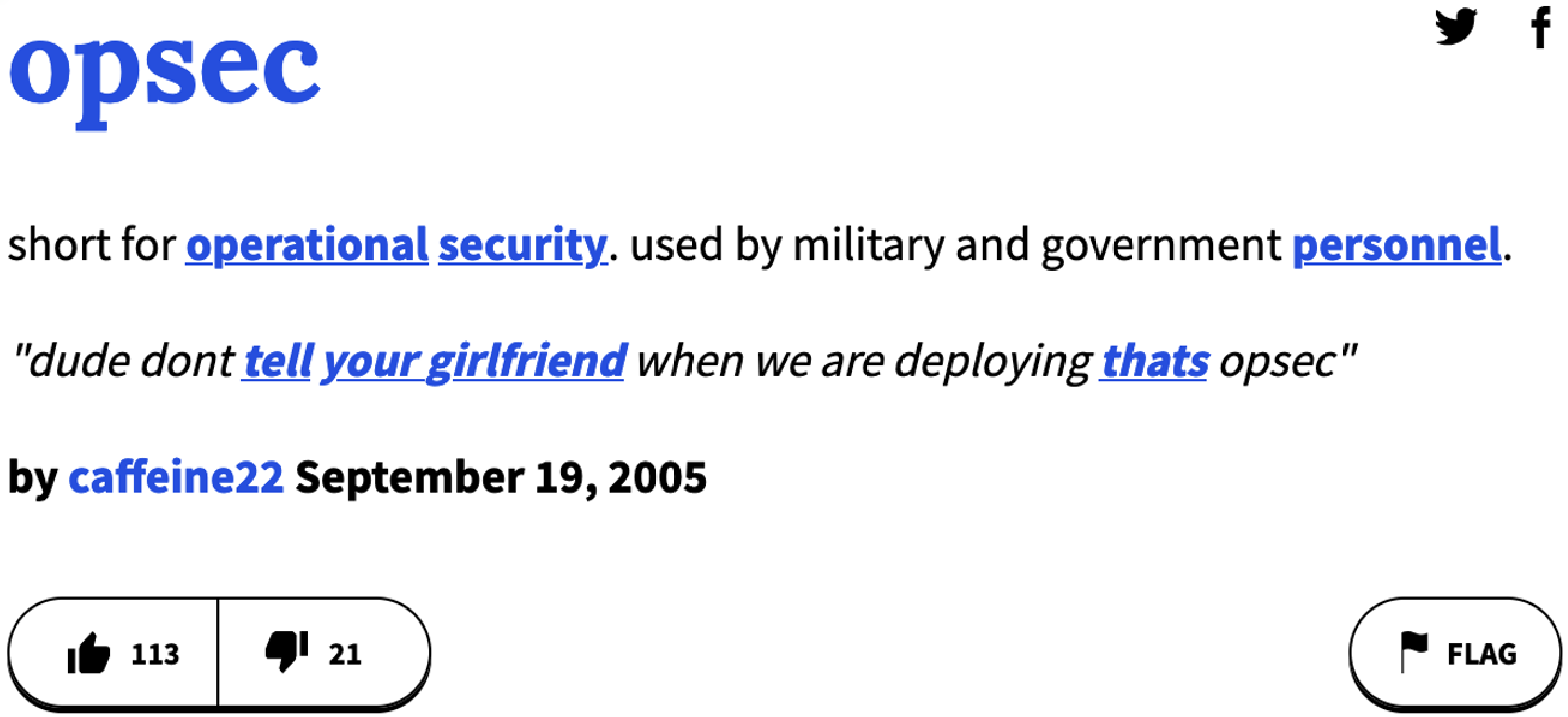
Sources:
CNSSI 4009-2015

Red Team

Red Teams are not attackers. They are simulated attackers. Therein lies a huge difference. While all of InfoSec has a "candidate shortage" for all the open positions, there are always lines out the door and around the block for red team jobs. Maybe it's Hollywood delusions of grandeur. Yes, it's a cool job (I love my job and my team), but some red team candidates may need to check their motives for doing this kind of work.

With motives properly checked, we can remember that as simulated attackers, we are really still defenders. We pretend to be attackers. We mock up attack scenarios. The best of us go to great lengths to look like the real thing, and their stories inspire me and my team to go further as well. But we are still defenders. We have responsibilities to our employers, our clients/customers, our stakeholders, and the consumers/employees whose data is the treasure we chase and loot.

https://malcomvetter.medium.com/responsible-red-teams-1c6209fd43cc

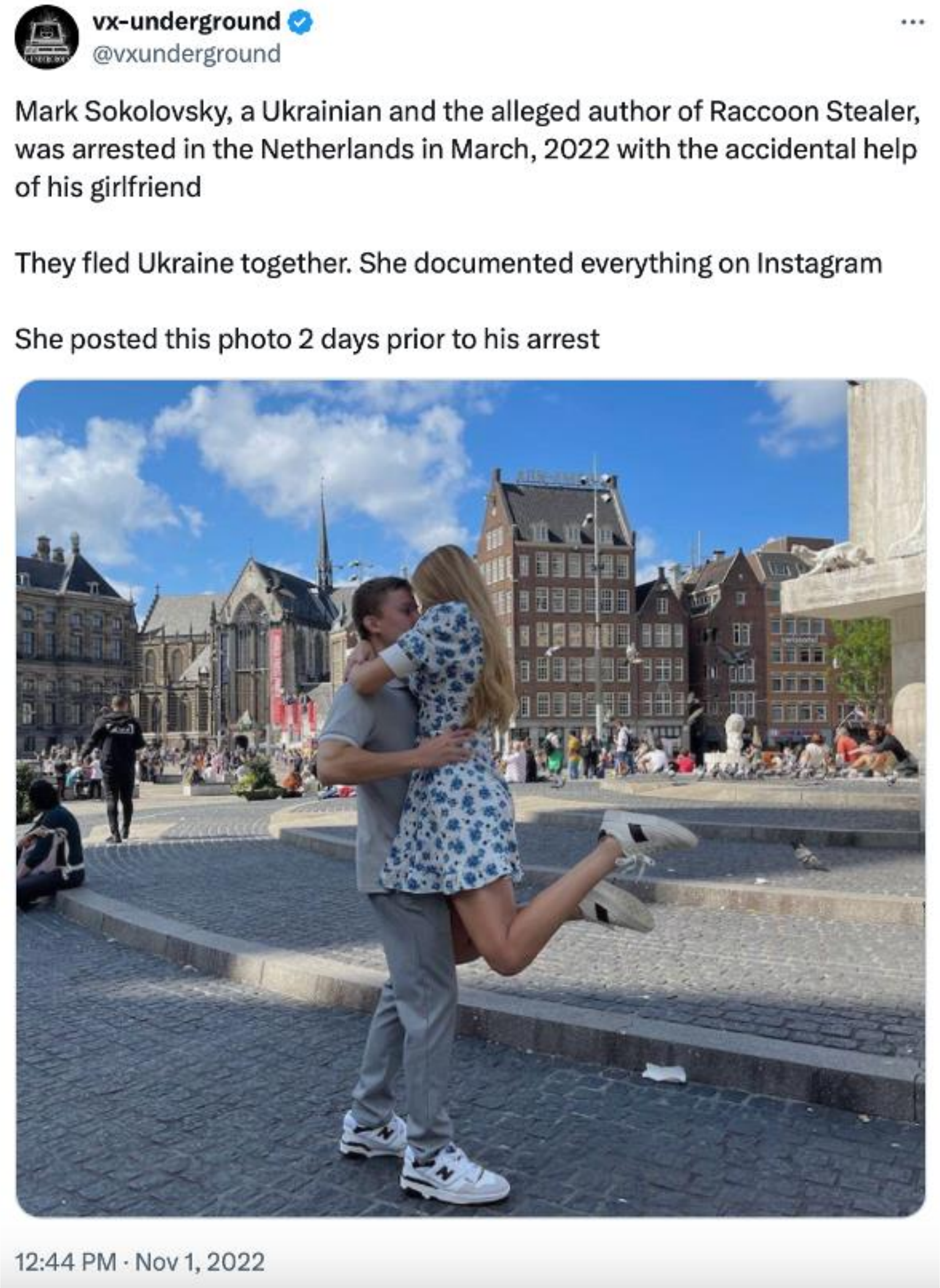


opsec

short for operational security. used by military and government personnel.

"dude dont tell your girlfriend when we are deploying thats opsec"

by caffeine22 September 19, 2005



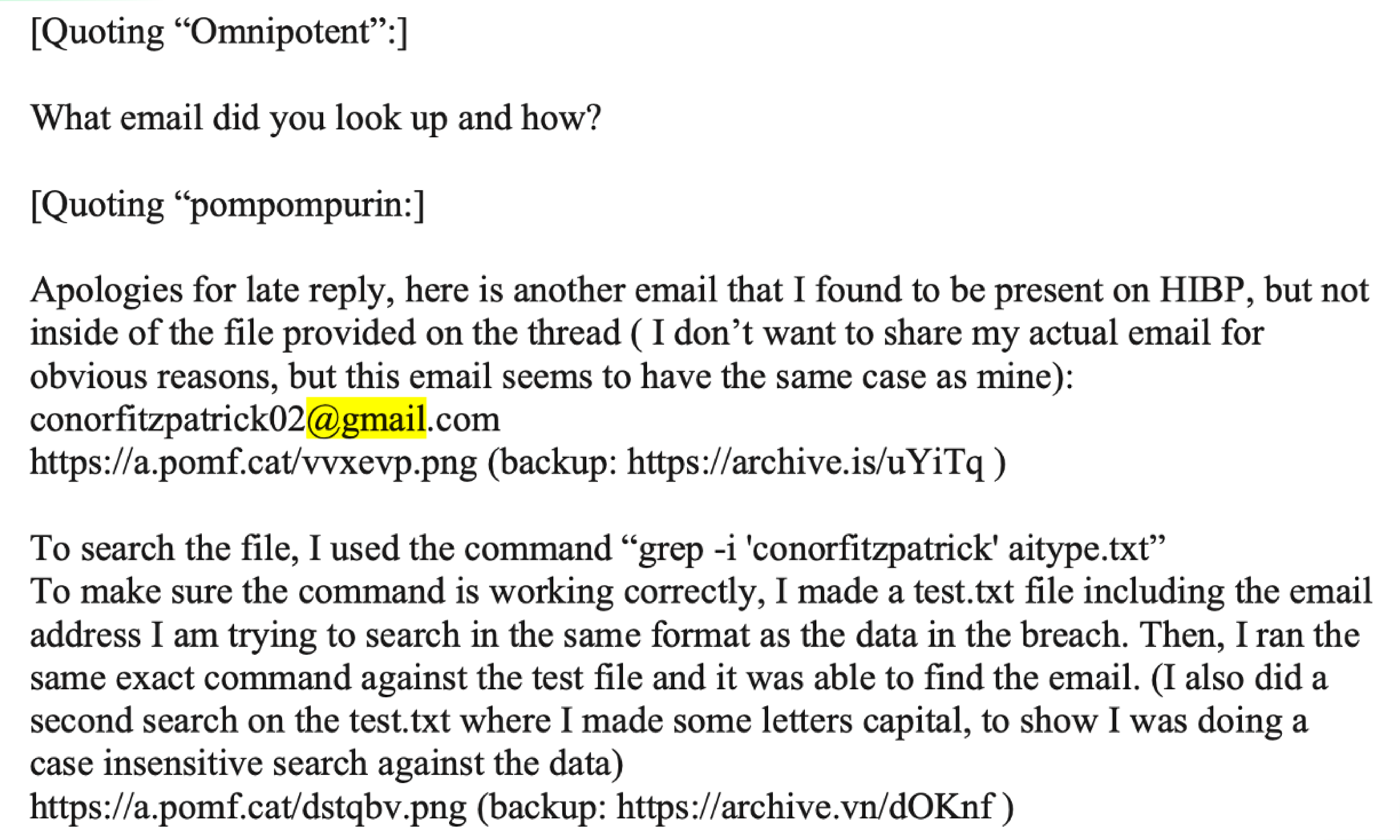
vx-underground
@vxunderground

Mark Sokolovsky, a Ukrainian and the alleged author of Raccoon Stealer, was arrested in the Netherlands in March, 2022 with the accidental help of his girlfriend

They fled Ukraine together. She documented everything on Instagram

She posted this photo 2 days prior to his arrest

12:44 PM · Nov 1, 2022



[Quoting “Omnipotent”:]

What email did you look up and how?

[Quoting “pompompurin:]

Apologies for late reply, here is another email that I found to be present on HIBP, but not inside of the file provided on the thread (I don’t want to share my actual email for obvious reasons, but this email seems to have the same case as mine):
conorfitzpatrick02@gmail.com
https://a.pomf.cat/vvxevp.png (backup: https://archive.is/uYiTq)

To search the file, I used the command “grep -i 'conorfitzpatrick' aitype.txt”
To make sure the command is working correctly, I made a test.txt file including the email address I am trying to search in the same format as the data in the breach. Then, I ran the same exact command against the test file and it was able to find the email. (I also did a second search on the test.txt where I made some letters capital, to show I was doing a case insensitive search against the data)
https://a.pomf.cat/dstqbv.png (backup: https://archive.vn/dOKnf)

Why Operational Security?

- **A red team engagement focuses on testing detection and response**
- **Try to not get caught**
  - Know what your tool does and what it leaves behind
  - Track and remove indicators of compromise
  - Ascertain that each action will provide value
    - Do I really need to run whoami? Is there an alternate way?
- Indicators of malicious activity are well known
- Blue teams have access to many sources that informs them of malicious activity
  - ”Threat Intel”
  - ”Google”
  - “Twitter”
  - ”PITSF”

Five-step OPSEC Process

1. **Identify sensitive data** - understand what your sensitive information might be.
2. **Threat Assessment** - identify potential cybersecurity threats, i.e., think of what adversaries could exploit about you.
3. **Vulnerability analysis** - identify where you are vulnerable and/or weaknesses in security.
4. **Risk assessment** - measure the level of risk to do with each previously identified vulnerability.
5. **Apply countermeasures** - develop countermeasures to minimize the identified risks.

https://www.sans.org/blog/what-is-opsec/

General Decision-Making Guide

1. **What is the objective?**
2. **How can we achieve the objective?**
    - For each action leading to that objective, what does it leave?
    - Will the information once investigated, point to the red team?
3. **Adjust accordingly to mitigate the risks of information disclosure**

Active Directory Attack Cycle

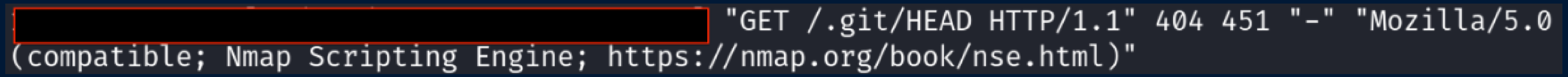
1. **Initial Access**
2. ~~Persistence~~
3. ~~Local Privilege Escalation~~
4. **Domain Enumeration**
5. **OS Credential Dumping**
6. **Lateral Movement**
7. **Domain Privilege Escalation**

Initial Access

- **Several ways to gain initial access**
  - Social Engineering *(*shing)*
  - Login from a publicly exposed service
  - Exploitable publicly facing service
  - Internal rouge devices
  - Supply chain attacks
  - Initial access is "difficult" these days
- **Security tooling has improved a lot**
  - Prevention and detection
- **Infrastructure can get you caught**

OPSEC Considerations: Initial Access

- **Secure your hosts**
- **Allowlist IPs**
- **Default User-Agents**
- **Source IP Addresses**
- **Tool-specific IOCs**
  - GoPhish’s “?rid” and “X-Mailer GOPHISH”
  - Evilginx’s “x-evilginx” header



```
[redacted] "GET /.git/HEAD HTTP/1.1" 404 451 "-" "Mozilla/5.0
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

Initial Access: Scenario 1

1. The red team performs external reconnaissance on the target organization from Source IP Address A.
2. The blue team detects the conducted port scan.
3. A few days later, the red team sends out a phishing email coming from Source IP Address A.

What could happen next?

Initial Access: Scenario 2

1. The target organization has offices in the Philippines and Singapore.
2. The red team successfully phished a user and logged in using those credentials from Vietnam.
3. The blue team receives an alert from that login.

What could happen next?

Domain Enumeration

- **Gather as much information as we can to identify interesting**
    - Users, groups, memberships, ACLs, trusts, configurations, etc.
- **Network Discovery**
    - DNS, targeted port scans
- **The goal is to learn as much as we can and still blend with the environment**
- **Next steps will build on the information gathered here**
    - Username format, key servers (computer name format), services used for remote administration
- **Can attract Blue Team attention very quickly**

OPSEC Considerations: Domain Enumeration

- **Gathering a full picture of the domain can be very noisy**
  - Hello, Bloodhound
- **Use of attacker tooling will of course require you to bypass endpoint protection, but they may work**
  - PowerView / SharpView
- **Ideally, use tooling that are built-in**
  - If on a server - AD Module? DSQuery?
  - Net commands? NLTest?
- **Keep watch of novel methods**
  - Active Directory Web Services (ADWS): https://www.mdsec.co.uk/2024/02/active-directory-enumeration-for-red-teams/

Domain Enumeration: Scenario

1. The red team successfully compromised a regular domain user with default privileges.
2. The red team’s current tradecraft bypasses endpoint protection and uses SharpView for targeted domain enumeration.
3. The Blue team does not currently detect the ongoi gdomain enumeration.

What will you do next?

1. Continue targeted domain enumeration
2. Take a break and go for a coffee

OS Credential Dumping

- "Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password. Credentials can be obtained from OS caches, memory, or structures.”
- **Extracted credentials can be used to**
  - Compromise another user
  - Gain access to a new host / service
  - Elevate domain privileges
- **Current Windows detection mechanisms plus endpoint protection makes it difficult to dump credentials**
  - Command line is logged
  - Process access is logged
  - LSASS, NTDS.dit

OPSEC Considerations: OS Credential Dumping

- **Do you really need to touch LSASS?**
  - What about plaintext credentials in scripts, config files?
  - Credential reuse? Tickets? Tokens? Cached Credentials?
- **DCSync**
  - Domain controllers replicate to each other for availability purposes
  - Done via Directory Replication Service Remote (MS-DRSR) protocol
  - This traffic only happens between domain controllers
    - MS-DRSR traffic between a workstation and DC?
  - Do you need to dump credentials of all users?
- NTDS.dit file
  - ntdsutil, Backup Operators Group, VSS

OS Credential Dumping: Scenario

1. The red team successfully escalated their privileges to Domain Admin (DA) but needs credentials for a specific account to login to a service.
2. The red team used Mimikatz’s “DCSync” capability to retrieve this credential using a newly created DA account.

What could happen next?

Lateral Movement

- “…techniques that adversaries use to enter and control remote systems on a network… Reaching their objective often involves pivoting through multiple systems and accounts to gain..”
- **There are several avenues for lateral movement**
    - Manipulating network traffic
    - Internal spear phishing
    - Using credentials and remote services to compromise new hosts
- **From leaving traces only on one host, now you are leaving traces on two**
    - PsExec, WMI, RDP, SSH, etc.

OPSEC Considerations: Lateral Movement

- **Use services that are used by the organization**
  - Nature, culture, maturity
- **Is that account used to login to that service?**
- **Windows-based tools vs Linux-based tools**
  - PsExec.exe vs Impacket’s psexec vs. Metasploit’s psexec
  - What artifacts do they leave?
- **Which user are you currently running your commands as?**

Lateral Movement: Scenario

1. The red team compromised an account that can login via PowerShell Remoting on one of the organization's key servers.
2. The red team used the **“Invoke-Command”** cmdlet to remotely load and execute a PowerShell-based enumeration script.

What could happen next?

Domain Privilege Escalation

- **Gaining administrative privileges is often required to achieve red team objectives**
- **End goal is often associated with gaining "DA"**
  - Not always necessary
- **Most likely deal with Kerberos-based attacks**
  - Understanding how Kerberos works is important
- **Several attacks to escalate privileges - choose wisely**
  - With enough monitoring, you will stand out

OPSEC Considerations: Domain Privilege Escalation

- **Do you know how cool stuff works?**
  - Golden ticket, ten years validity?
  - Kerberos everything? RC4 encryption type?
- **Use services that are used by the organization**
  - Do they use PowerShell Remoting? RDP?
- **Do you really need ”DA”?**
- **Minimize changes**

Domain Privilege Escalation: Scenario

1. The red team is looking for an account that is vulnerable to Kerberoasting.
2. The red team used Rubeus, a C# toolset for Kerberos interaction.
3. The red team requested several RC4 encrypted TGS tickets for several services.

What could happen next?

CONCLUSION

- **Being a red team operator is highly technical, stressful, and requires you to be up-to-date**
  - "You vs a multi-billion organization"
- **Your tradecraft will be a limiter**
  - Trainings
  - Research
  - Teammates
- **Your target organization's capabilities will be a limiter**
  - No organization is the same - some will be great, some will suck
- **Newton's Third Law**
  - "For every action there is an equal and opposite reaction."

REFERENCES

- Ethical Hacking Model
- What is OPSEC?
- https://www.justice.gov/usao-edva/file/1300536/dl
- https://blogs.blackberry.com/en/2023/01/cybercriminal-faked-death-found

Thank You

ROOTCON18 Red Teaming Village