RED TEAMING

«LA SIMULAZIONE DI ATTACCHI INFORMATICI COME METRICA DI VALUTAZIONE»

Stefano Maccaglia
Global Practice Manager Netwitness Incident Response

Paolo Coba
Senior Consultant Netwitness IR Red Team

ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Who we are: Stefano

- I am the Global Manager for the Netwitness Incident Response Team.
- I begun my ICT career in 1997 in Digital Corp, but I started to crack software in 1985 with a Commodore C64…
- I decided to get out of the cracking scene in 2000 and for about three years I remained focused on Networking and System administration… until Nimda and Blaster came out and testing network and system security became an interesting career…
- I worked on the testing and offensive side until 2009 when I jumped into the IR bandwagon.
- I currently manage the IR and RT practice for Netwitness.

Who we are: Paolo

- I am a Senior Consultant for Netwitness.
- I begun my career in programming for mobile and web applications, but decided to join cybersecurity after I completed my University curricula.
- I joined the Netwitness IR practice in 2021 as an IR analyst and I started developing my Offensive skills almost ever since.
- Currently I am part of Netwitness Red Team: “the Shadow Wolves”.

Who we are

- Shadow Wolves are a team, inside Netwitness IR Practice, dedicated to Red Teaming activities.
- These activities involve:

Threat Modeling

We analyze systems and networks to identify potential threats, vulnerabilities, and risks.

Security Architecture Review

We evaluate security architectures, including network and security designs, access controls, and segmentation.

Zero-day Exploit Testing

We assess resilience to zero-day exploits, which are vulnerabilities unknown to software vendors or unpatched.

Adversarial Simulation

We simulate TTPs of real-world threat actors, such as advanced persistent threats (APTs) evaluating visibility and breach readiness.

Agenda

What is Red Teaming

Red Teaming Vs Penetration Testing

How Red Teaming is planned and executed

An example of Red Teaming planning

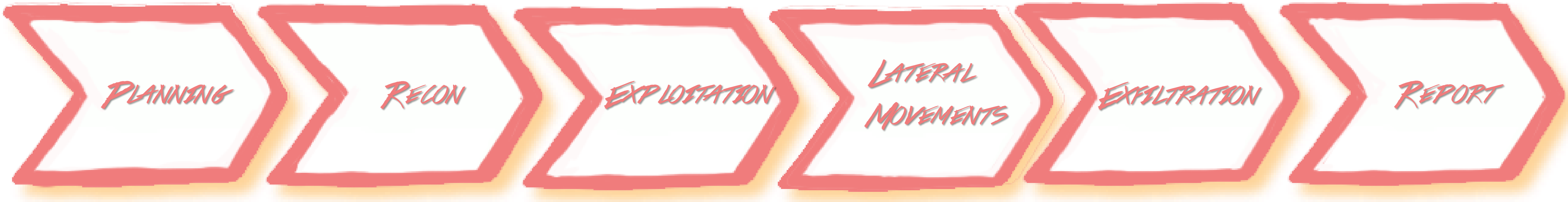
Examples of exploitation techniques used in Red Teaming

Metrics to evaluate Incident Readiness

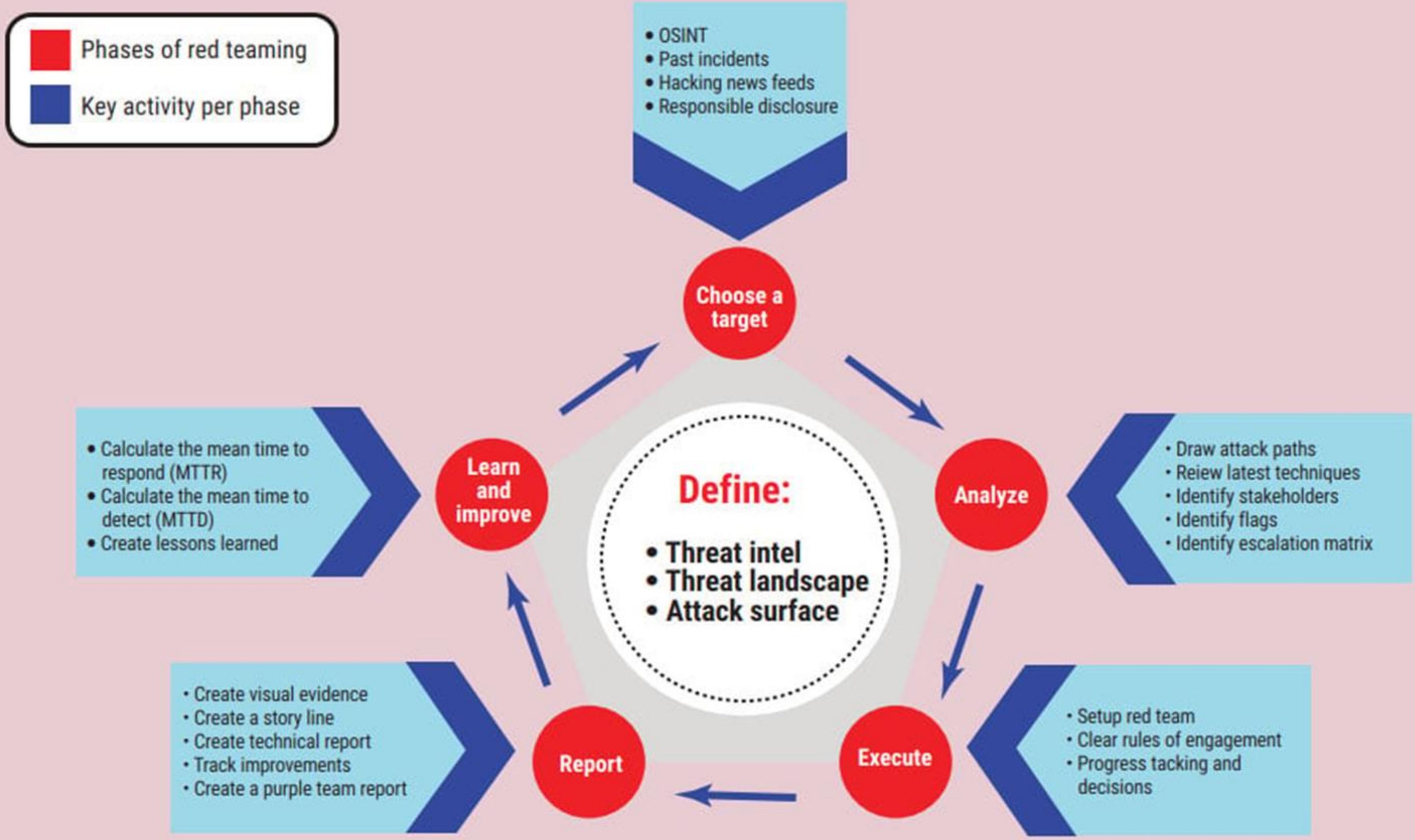
Conclusions

What is Red Teaming?

- Red teaming is a proactive approach to cybersecurity assessment aimed at identifying vulnerabilities within an organization's systems, processes, and people
- Unlike traditional penetration testing, which focuses on finding and fixing specific vulnerabilities, red teaming simulates real-world cyberattacks to assess an organization's overall security posture.



Red Teaming overview



- 🟥 Phases of red teaming
- 🟦 Key activity per phase

Define:

- Threat intel
- Threat landscape
- Attack surface

Choose a target

- OSINT
- Past incidents
- Hacking news feeds
- Responsible disclosure

Analyze

- Draw attack paths
- Reiew latest techniques
- Identify stakeholders
- Identify flags
- Identify escalation matrix

Execute

- Setup red team
- Clear rules of engagement
- Progress tacking and decisions

Report

- Create visual evidence
- Create a story line
- Create technical report
- Track improvements
- Create a purple team report

Learn and improve

- Calculate the mean time to respond (MTTR)
- Calculate the mean time to detect (MTTD)
- Create lessons learned

Red Teaming Vs Penetration Testing

GOALS

Simulate real-world cyberattacks by adopting the mindset and tactics of a malicious actor.

Identify and exploit specific vulnerabilities within an organization's systems, networks, or applications.

TARGETS

Simulate multi-stage attacks to evaluate an organization's overall security posture and resilience.

Penetration tests are narrowly scoped, focusing on specific systems, applications, or network segments identified by the organization as potential targets.

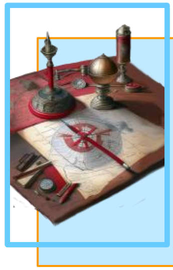
METHODOLOGY

Holistic approach, emulating the tactics, techniques, and procedures (TTPs) of real adversaries. Red teamers may employ a combination of TTPs to achieve their objectives.

Penetration tests follow a structured and systematic approach, focusing on identifying and exploiting known vulnerabilities.

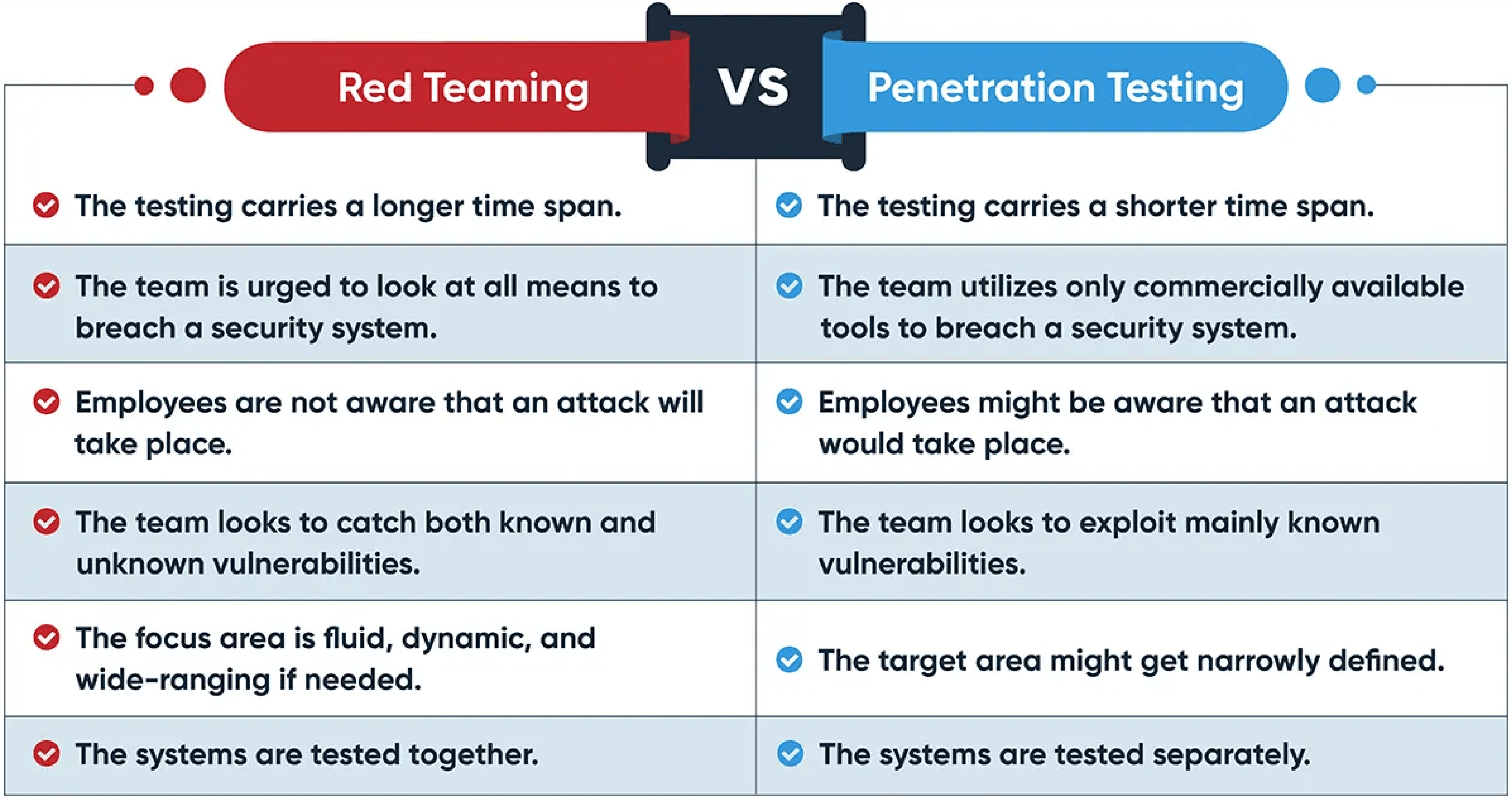
REPORTING

The assessment culminates in detailed reports that document the TTPs used during the engagement, as well as the vulnerabilities exploited and recommendations for improvement.



Report typically focuses on the specific vulnerabilities identified and exploited during the assessment, along with recommendations for remediation.

In a nutshell…



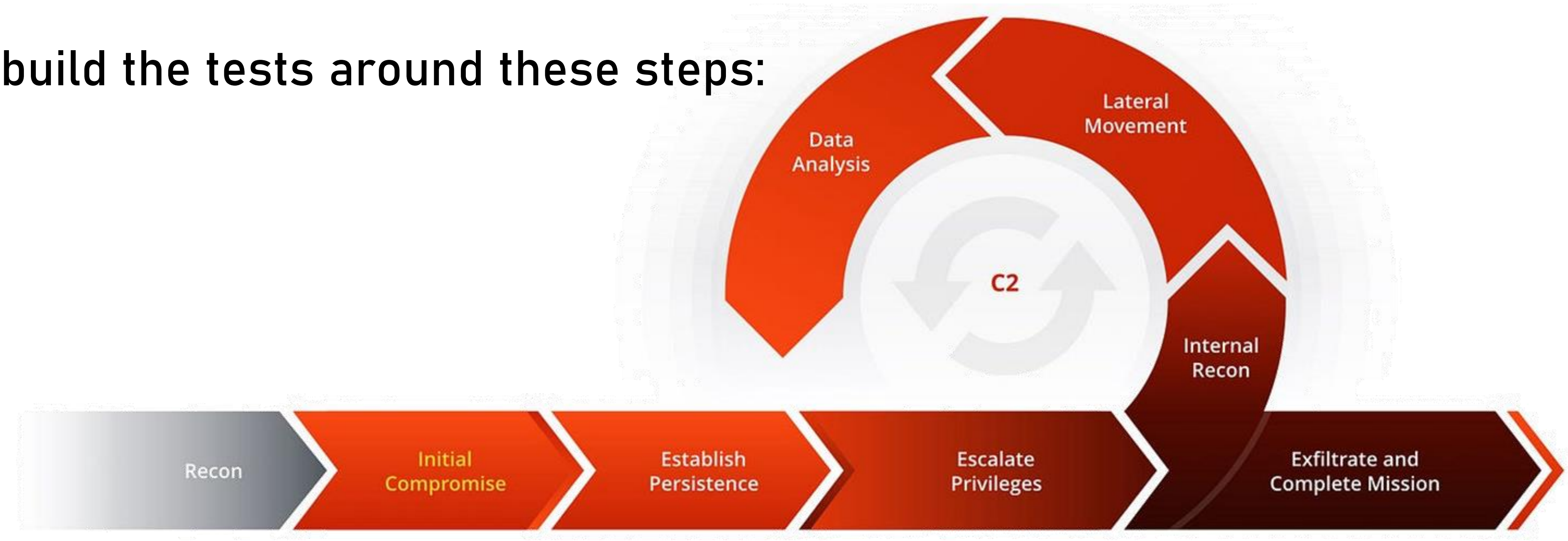
Red Teaming	Penetration Testing
The testing carries a longer time span.	The testing carries a shorter time span.
The team is urged to look at all means to breach a security system.	The team utilizes only commercially available tools to breach a security system.
Employees are not aware that an attack will take place.	Employees might be aware that an attack would take place.
The team looks to catch both known and unknown vulnerabilities.	The team looks to exploit mainly known vulnerabilities.
The focus area is fluid, dynamic, and wide-ranging if needed.	The target area might get narrowly defined.
The systems are tested together.	The systems are tested separately.

It's a draw…

- While both red teaming and penetration testing play essential roles in assessing and improving an organization's cybersecurity posture, they differ in their objectives, scope, approach, and frequency.
- Red teaming provides a comprehensive and realistic assessment of an organization's security defenses against advanced threats, while penetration testing focuses on identifying and remediating specific vulnerabilities within a defined scope.
- Depending on the organization's goals, risk tolerance, and resource availability, a combination of red teaming and penetration testing may be employed to achieve a robust and proactive cybersecurity strategy..

How Red Teaming is executed?

- We build the tests around these steps:

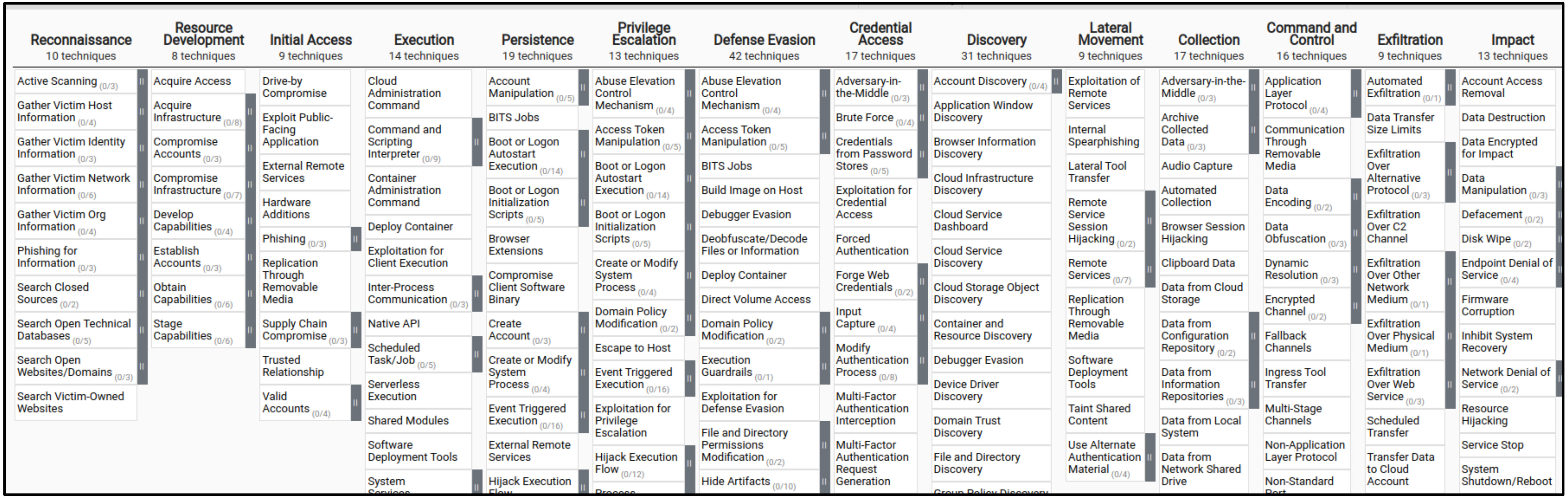


- We use MITRE ATT&ck Framework to design and emulate real actors.
- In a typical engagement, we define the TTPs, review the attacker toolset and then shape the simulation around these items.

Note: for limited activities, not aimed to fully execute an attack, we usually adopt the "assumed breach" condition, meaning our analyst start acting from an already controlled machine.

MITRE ATT&ck Framework in Red Teaming

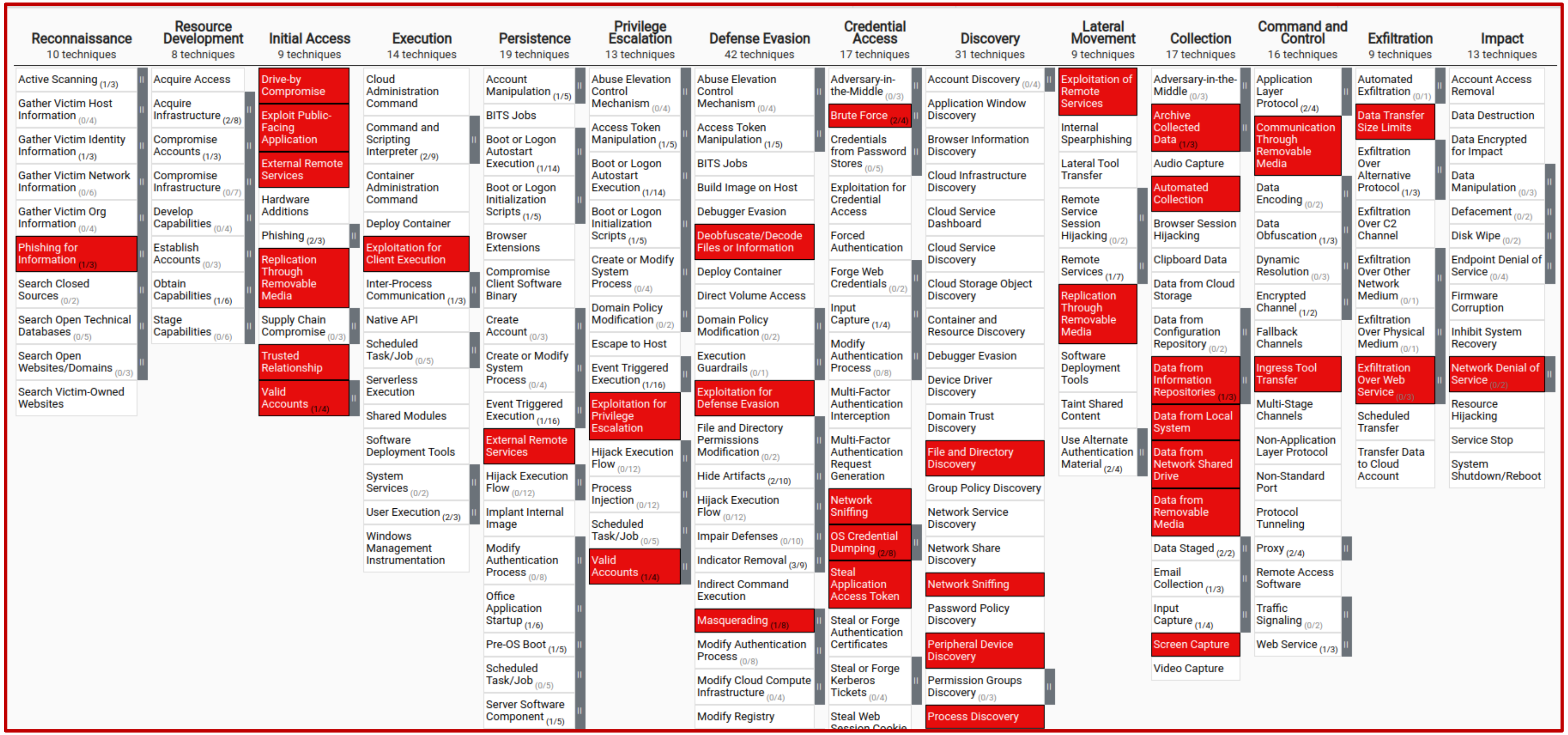
- We use MITRE framework to define the techniques to adopt.
- It supports the Customer when reading our final report.



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Exploit Public-Facing Application	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Phishing (0/3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/7)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Establish Accounts (0/3)	Replication Through Removable Media	Inter-Process Communication (0/3)	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/6)	Supply Chain Compromise (0/3)	Native API	Create Account (0/3)	Escape to Host	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (0/3)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Trusted Relationship	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Direct Volume Access	Modify Authentication Process (0/8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Serverless Execution	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Shared Modules	External Remote Services	Hijack Execution Flow (0/12)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
			Software Deployment Tools	Hijack Execution Flow	Process	Exploitation for Defense Evasion		Domain Trust Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			System Services			File and Directory Permissions Modification (0/2)		File and Directory Discovery					Service Stop
						Hide Artifacts (0/10)		Group Policy Discovery					System Shutdown/Reboot

Mapping Tactics & Techniques

- By mapping the real used techniques, the Team can build the scenario and can decide what tool to adopt to emulate the outcome of the attacker tools.



Reconnaissance
10 techniques

- Active Scanning (1/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (1/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (2/8)
- Compromise Accounts (1/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (1/6)
- Stage Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (2/9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (1/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (2/3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (1/5)
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (1/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (1/16)
- External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/8)
- Office Application Startup (1/6)
- Pre-OS Boot (1/5)
- Scheduled Task/Job (0/5)
- Server Software Component (1/5)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (1/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (1/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (1/4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (2/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (0/10)
- Indicator Removal (3/9)
- Indirect Command Execution
- Masquerading (1/8)
- Modify Authentication Process (0/8)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry

Credential Access
17 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (2/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (1/4)
- Modify Authentication Process (0/8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (2/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie

Discovery
31 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (1/7)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (2/4)

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (1/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (1/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2/2)
- Email Collection (1/3)
- Input Capture (1/4)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (2/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (1/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (1/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (2/4)
- Remote Access Software
- Traffic Signaling (0/2)
- Web Service (1/3)

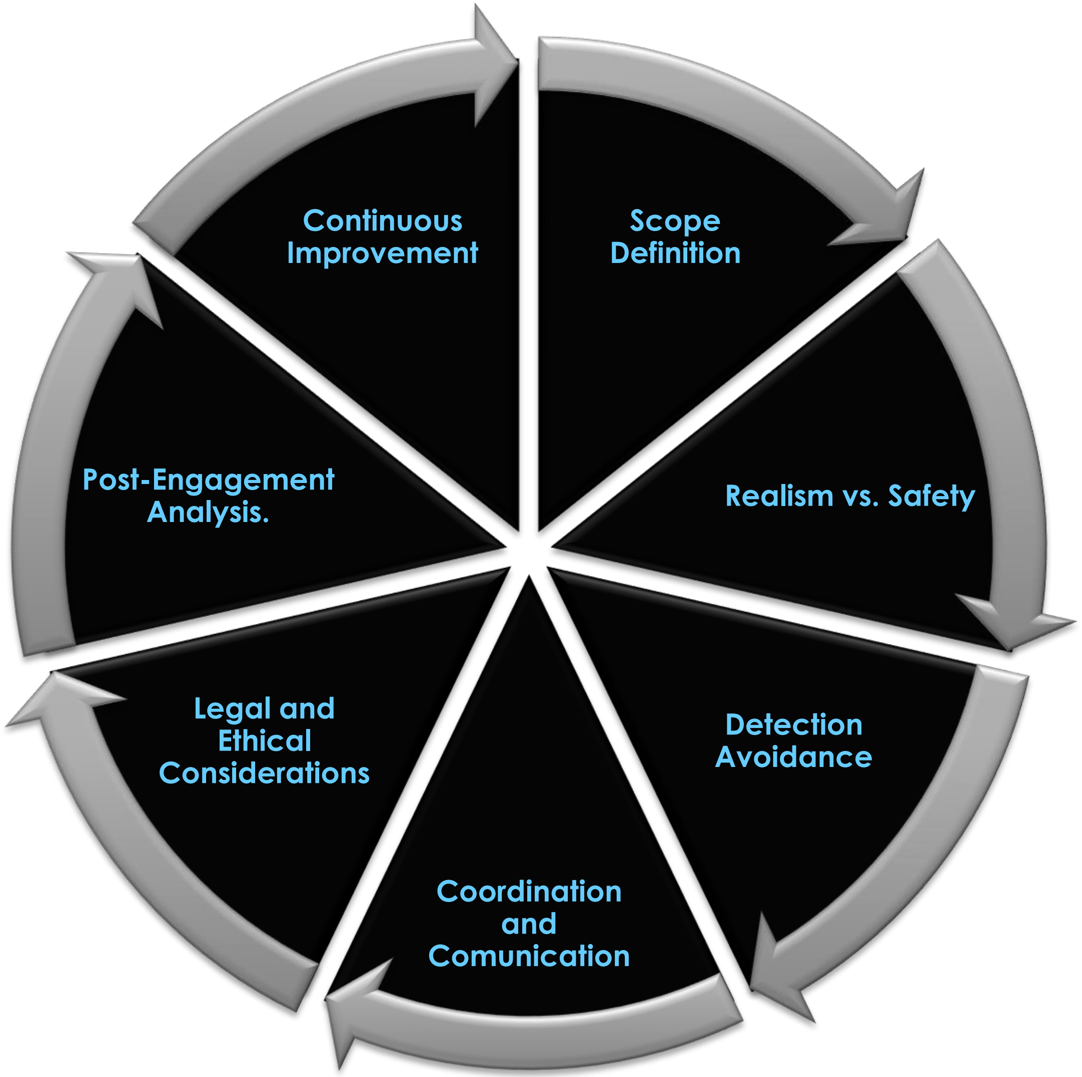
Exfiltration
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (1/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/3)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

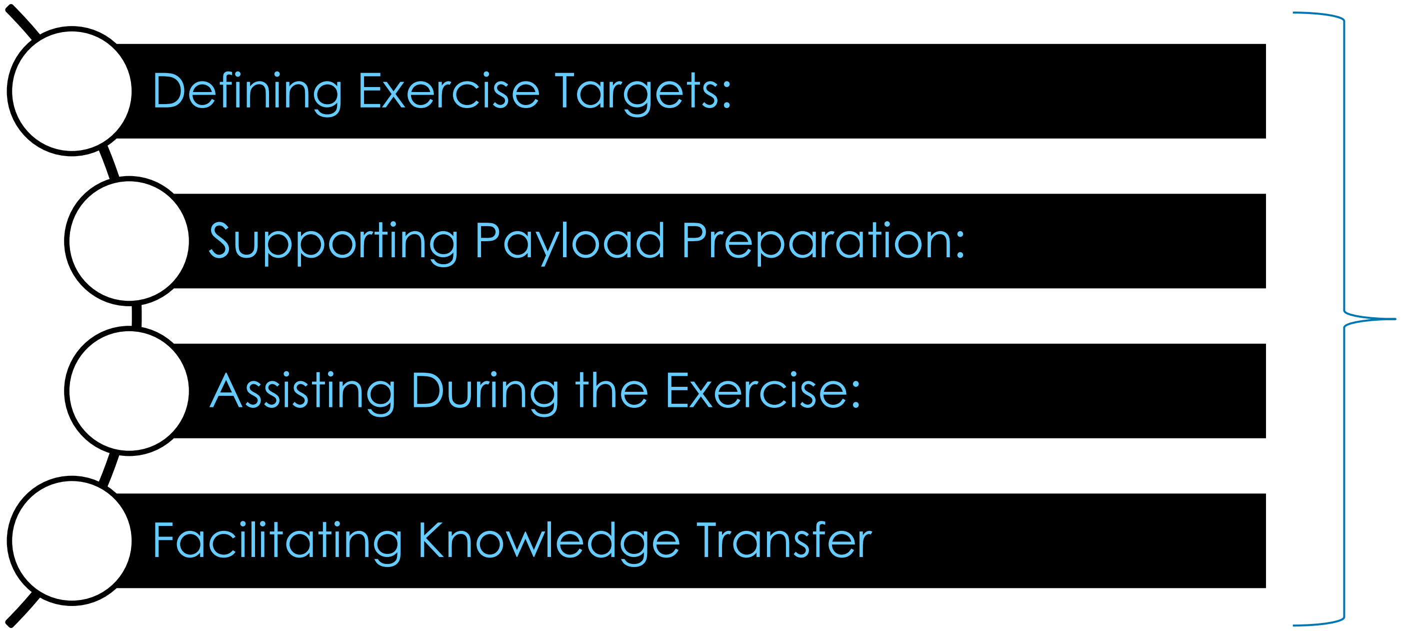
Red Teaming Challenges



Scope Definition
Realism vs. Safety
Detection Avoidance
Coordination and Comunication
Legal and Ethical Considerations
Post-Engagement Analysis.
Continuous Improvement

A Key role: Internal Referrer (Internal Support Engineer)

- The internal engineer supporting the Red Team plays a crucial role in ensuring the success and effectiveness of red team exercises:



Defining Exercise Targets:
Supporting Payload Preparation:
Assisting During the Exercise:
Facilitating Knowledge Transfer

The Internal Referrer plays a pivotal role for his technical expertise, familiarity with the organization's infrastructure.

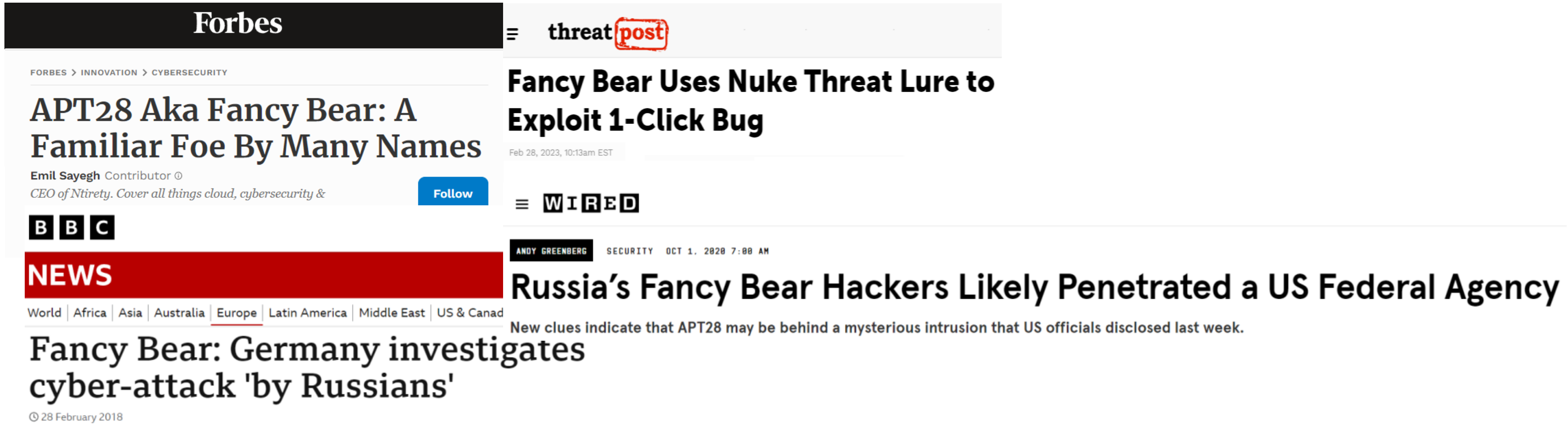
- A strong collaborative approach is essential for maximizing the effectiveness and value of test in identifying and mitigating security risks.

An example

APT 28 (aka Fancy Bear)

- APT28, also known as Fancy Bear, is a sophisticated advanced persistent threat group associated with various cyber espionage campaigns.
- APT28 employs a range of tools and techniques to carry out their operations.

- By simulating an APT28 attack, we provide valuable insights into an organization's security strengths and weaknesses, helping to enhance its defenses against such a menace.



Forbes

FORBES > INNOVATION > CYBERSECURITY

APT28 Aka Fancy Bear: A Familiar Foe By Many Names

Emil Sayegh Contributor

CEO of Ntirety. Cover all things cloud, cybersecurity &

Follow

threatpost

Fancy Bear Uses Nuke Threat Lure to Exploit 1-Click Bug

Feb 28, 2023, 10:13am EST

BBC

NEWS

World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canad

Fancy Bear: Germany investigates cyber-attack 'by Russians'

28 February 2018

WIRED

ANDY GREENBERG SECURITY OCT 1, 2020 7:00 AM

Russia's Fancy Bear Hackers Likely Penetrated a US Federal Agency

New clues indicate that APT28 may be behind a mysterious intrusion that US officials disclosed last week.

APT 28 typical tools

- APT28 developed a remarkable arsenal of custom tools.

Sofacy/Seduploader

- Sofacy is a custom-made downloader tool used to deliver additional malware.

XAgent

- XAgent is a modular backdoor.

XTunnel

- XTunnel is another tool developed to establish a covert communication channel between the compromised system and the attacker's C2 server

Chopstick

- It is a modular toolkit that enables APT28 operators to deploy a variety of plugins and tools on compromised systems.

Gamefish

- Gamefish, is a custom backdoor primarily used to target government entities and diplomatic organizations.

Zebrocy

- Zebrocy is a reconnaissance tool delivered via spear-phishing emails containing malicious Microsoft Office documents.

- It's important to note that any APT threat constantly evolves his toolkit and may employ new or modified tools to stay ahead of detection.
- Therefore, our Threat Intel team is constantly supporting us to remain up-to-date with most recent TTPs from this actor.

APT 28 attack strategies

Typical APT28 attack leverages on knowledge gained by the actor prior to target the victim.

- Two attack vectors are typically used by APT28 to initially target organizations.

Secondly, legitimate websites that are visited by potential targets can be compromised to deliver malicious code in watering hole attacks.

But even when APT28 exploits a server, the goal is to leverage on this system for watering-hole attacks, meaning he plans to use this compromised system to target users and to win user's trust.

Firstly, (spear) phishing can be used to initially send links to malicious URLs or to deliver malicious documents to specific targets.

Execution Phase

- The initial attack vectors are followed by three attack paths.

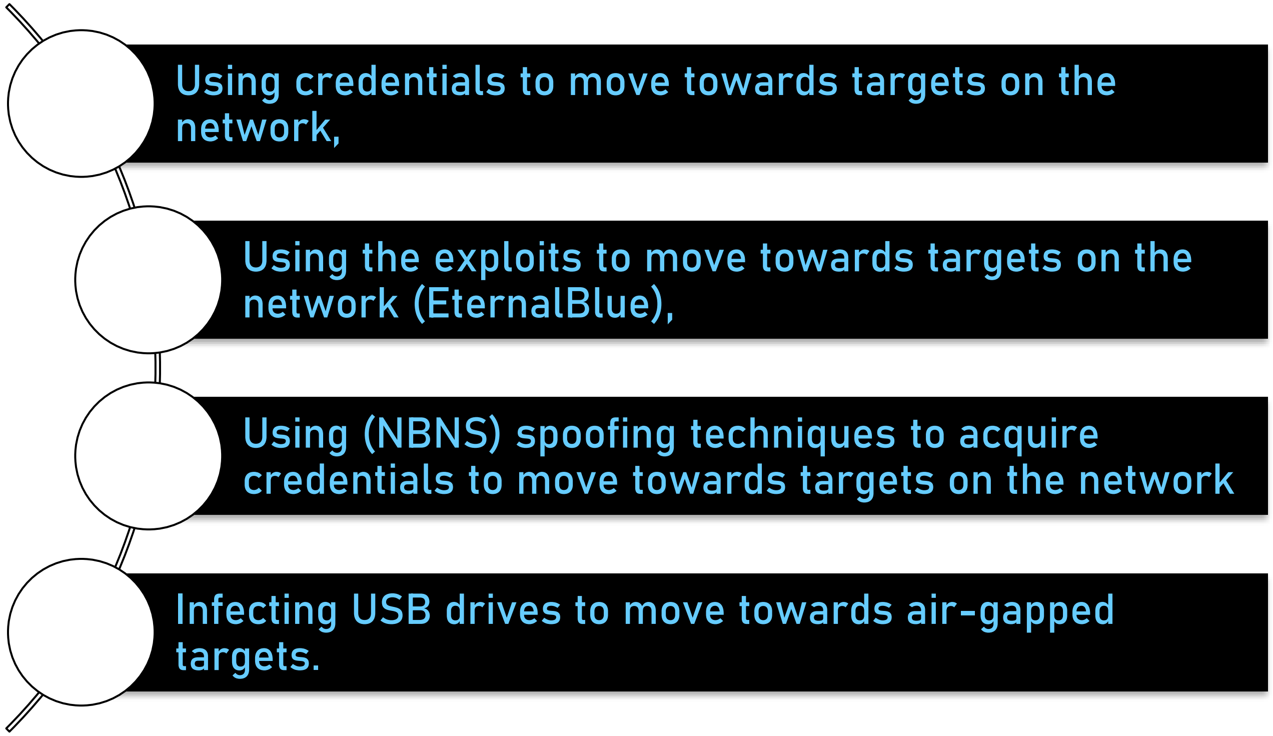
3 ACQUIRING CREDENTIALS

4 INFECTING SYSTEMS WITH FIRST STAGE MALWARE

5 INFECTING SYSTEMS THROUGH EXPLOITS.

Persistence and Lateral Movement

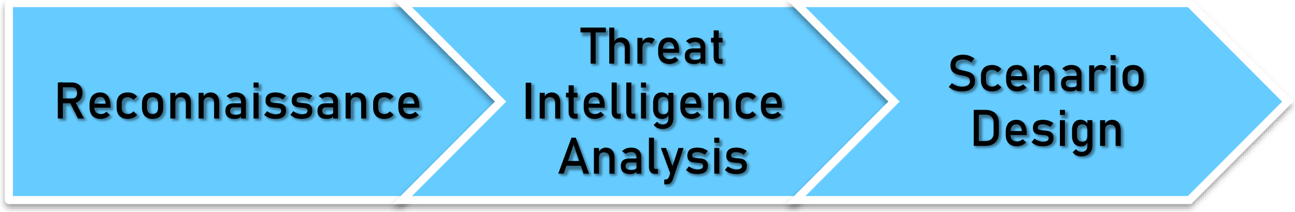
- Once APT 28 has deployed its malware to one system of a targeted organization, other (in)directly reachable internal systems of the organization may be targeted.



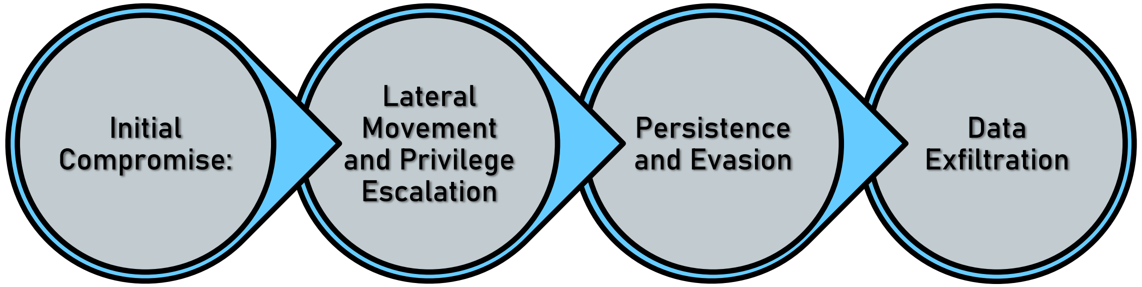
- Using credentials to move towards targets on the network,
- Using the exploits to move towards targets on the network (EternalBlue),
- Using (NBNS) spoofing techniques to acquire credentials to move towards targets on the network
- Infecting USB drives to move towards air-gapped targets.

Test Planning

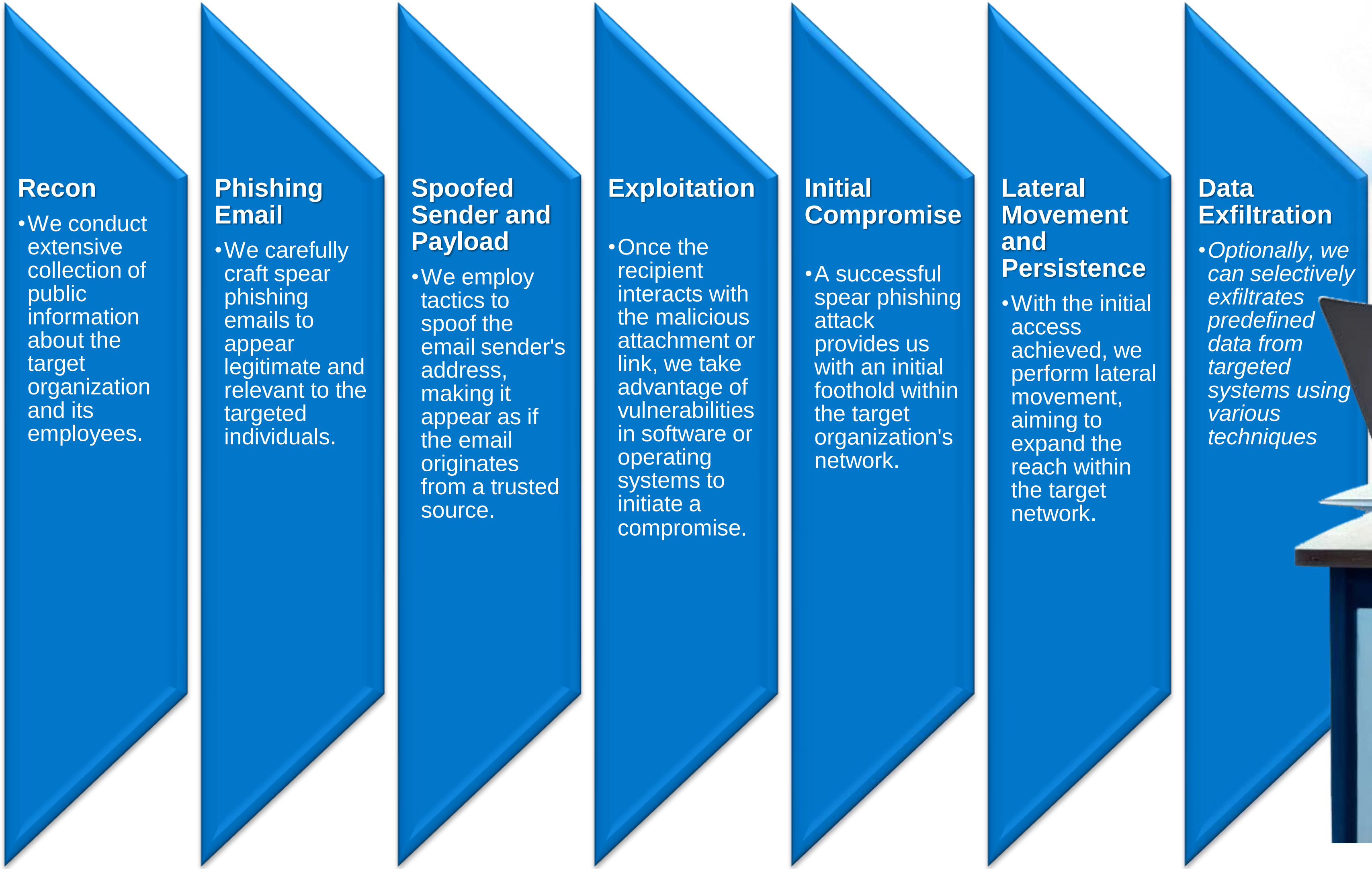
- The exercise aims to emulate TTPs associated with APT28.
- To do that we focus on the following steps:



- A typical test based on APT28 includes:



How we build the APT28 attack scenario



Recon

- We conduct extensive collection of public information about the target organization and its employees.

Phishing Email

- We carefully craft spear phishing emails to appear legitimate and relevant to the targeted individuals.

Spoofed Sender and Payload

- We employ tactics to spoof the email sender's address, making it appear as if the email originates from a trusted source.

Exploitation

- Once the recipient interacts with the malicious attachment or link, we take advantage of vulnerabilities in software or operating systems to initiate a compromise.

Initial Compromise

- A successful spear phishing attack provides us with an initial foothold within the target organization's network.

Lateral Movement and Persistence

- With the initial access achieved, we perform lateral movement, aiming to expand the reach within the target network.

Data Exfiltration

- *Optionally, we can selectively exfiltrates predefined data from targeted systems using various techniques*

ISACA® Sistemi informativi: averne fiducia e trarne valore Rome Chapter

What is an expected outcome?

Identification of Weaknesses and Vulnerabilities

Validation of Defenses and Controls

Assessment of Detection and Response Capabilities

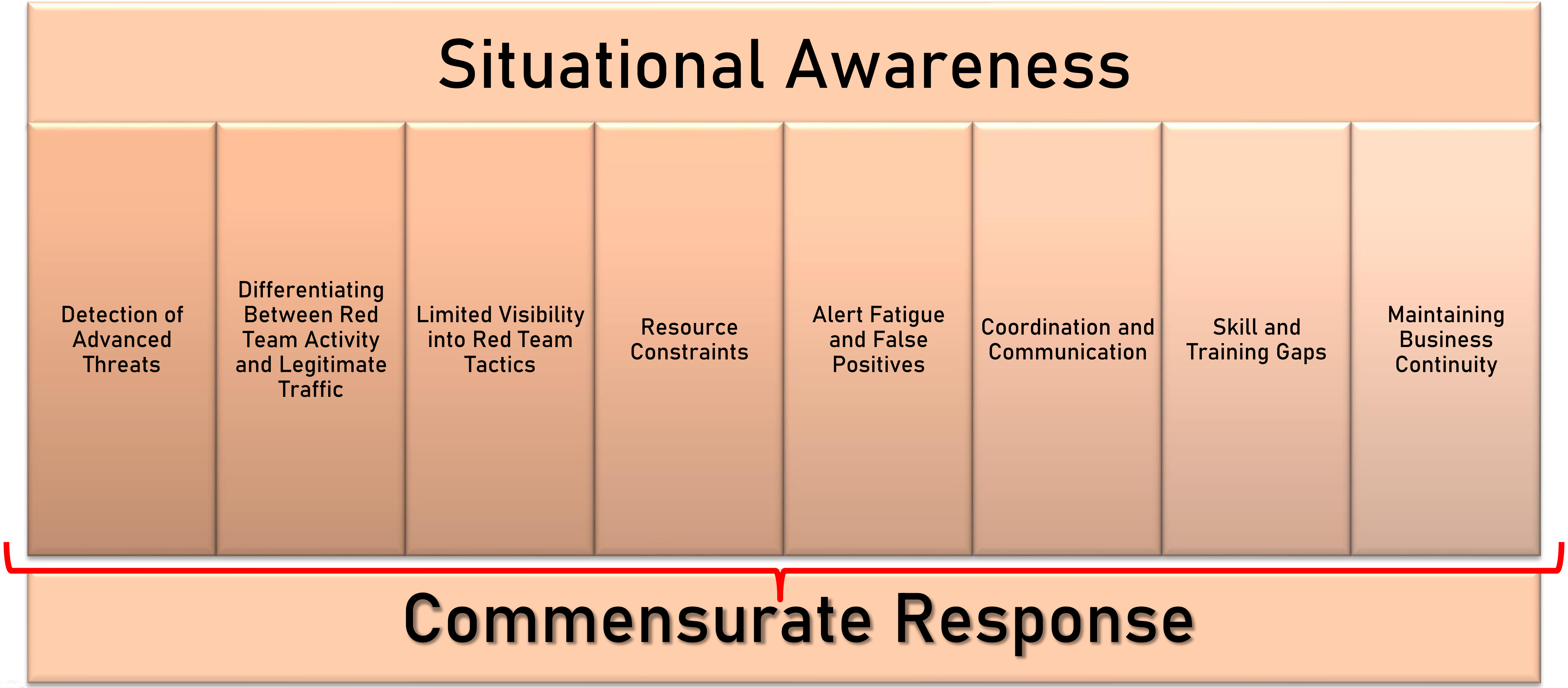
Enhanced Security Awareness and Training

Strategic Insights and Risk Prioritization

Continuous Improvement and Resilience Building

What is a typical challenge for the Blue Team?

- The blue team, responsible for defending against simulated cyberattacks during a red team test, faces several challenges. Here are some of the key challenges:



Situational Awareness

Detection of Advanced Threats

Differentiating Between Red Team Activity and Legitimate Traffic

Limited Visibility into Red Team Tactics

Resource Constraints

Alert Fatigue and False Positives

Coordination and Communication

Skill and Training Gaps

Maintaining Business Continuity

Commensurate Response

Visibility Vs Detectability

- The confrontation between visibility and detectability arises from the inherent challenge of collecting and analyzing large volumes of data to identify real security threats effectively.
- Organizations may have high visibility into their network and systems, capturing an extensive amount of data, but without the ability to effectively detect and respond to security incidents, that visibility is of limited value.
- Conversely, organizations may invest heavily in advanced detection technologies but without sufficient visibility into the environment, the detection capabilities will be severely hampered.

The technological pitfall…

- A common pitfall we found in our tests is the Blue team, and more in general the Company, relying too heavily on technologies…

- Complexity of the Threat Landscape
- Pace of Technological Innovation
- Limited Understanding of Adversarial Tactics
- Resource Constraints and Operational Pressures
- Vendor Marketing and Hype
- Complacency and False Sense of Security

How to avoid that pitfall?

- To mitigate these risks, the blue team should adopt a balanced approach to cybersecurity that combines technology, people, and processes.
- This includes investing in employee training and skill development, implementing robust processes and procedures, fostering a culture of security awareness, and continuously evaluating and evolving the organization's security posture to adapt to changing threats and technologies.
- By leveraging technology as part of a comprehensive defense strategy rather than relying on it exclusively, the blue team can better defend against

How to go beyond technologies

- Comprehensive Data Collection: Establishing robust monitoring mechanisms to capture relevant data across various network layers, endpoints, and applications.
- Centralized Log Management: Implementing centralized logging and log aggregation solutions to consolidate and manage the collected data efficiently.
- Security Analytics and AI: Leveraging advanced analytics, machine learning, and artificial intelligence techniques to analyze the collected data and detect patterns, anomalies, and potential threats.
- Threat Intelligence Integration: Incorporating threat intelligence feeds and utilizing up-to-date information on known attack techniques and IOCs to enhance detection capabilities.
- Incident Response Readiness: Establishing well-defined incident response processes and procedures to efficiently respond to detected security incidents and mitigate potential damage.

NETWITNESS
An RSA Business

Red Team Vs Production systems

Controlled	All techniques and payloads are controlled and tested in our labs with different OS versions and levels.
Stop before becoming disruptive	When a scenario is designed to be disruptive, we stop right before. (es. Ransomware)
Implants are not installed where not necessary	When the attack is designed, we avoid to target production systems for persistence, unless strictly needed (webshell).
Sensible data are not part of any actions	In the case of an exfiltration test, only dummy or common files will be considered.
Tests on copies	Whenever is possible. we request a copy of production operating systems for preliminary tests.

Red Team Vs Web Exploitation

TTPs

- On a production Web Server it is possible to install a webshell after an exploitation to gain the foothold.
- The communication with it will be secured as much as possible to avoid other interactions (password and encrypted sessions).
- Our team will avoid using any disruptive technique and will remove the artifacts upon the conclusion of the activity.

Red Team Vs Active Directory

TTPs

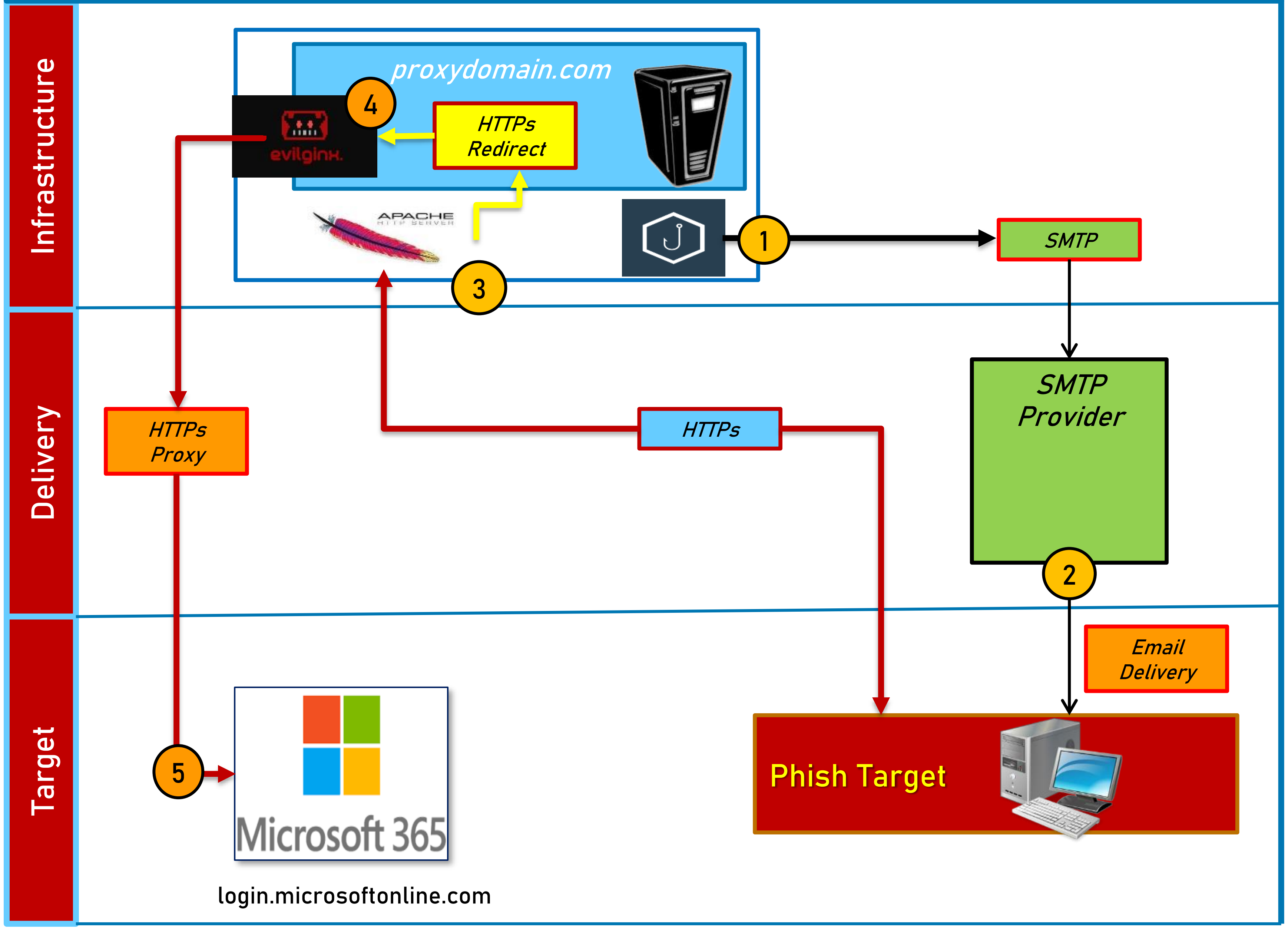
- Avoid using unstable exploits and invasive techniques (Zerologon).
- Captured credentials are used only for the activities conducted on in-scope systems.
- Focus on detecting and utilizing misconfigurations to elevate privileges on the domain.

Red Team Vs Cloud

TTPs

- When we test a Cloud infrastructure (e.g. IaaS), we treat it as the internal systems.
- When we test a Saas Cloud solution, our team approach it as an application server, and we are used to adopt the techniques focused on application exploitations.
- Traditionally, to target a Cloud is useful to acquire credentials through phishing and other social engineering techniques to obtain valid access tokens.
- Actions on Objectives are performed with administrative and native tools, mimicking APT behavior.

NW Phishing Infrastructure



Attack Scenario: Discovery

TTPs

- System Information Discovery (T1082)
- Account Discovery: Domain Account (T1087.002)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Remote System Discovery (T1018)
- Domain Trust Discovery (T1482)

Crucial phase for identifying as much information as possible about the target environment

Attack Scenario: Domain Escalation

TTPs

- ➢ Valid Accounts: Domain Accounts (T1078.002)
- ➢ Utilized Technique: Misconfigured Certificate Templates – ESC1

https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

Prerequisites

- ○ Enrollment rights granted to low-privilege users
- ○ No manager approval required
- ○ Requests can include subjectAltName

Result

- ✓ Permits low-privileged users to impersonate any domain principal.

Domain Admins are a great choice!!

Attack Scenario: Lateral Movement

TTPs

- Remote Services (T1021)

Technique 1: PowerShell Remoting

- Utilize built-in functionality to blend in the environment. Stealthier approach.

Technique 2: PsExec

- Utilize PsExec with a custom service executable to run an implant on the target system. Generates more noise.

Metrics, evaluation and Reporting

Metrics to assess the Incident Readiness

- When evaluating the effectiveness of a response during a Red Teaming test, it's essential to consider the following metrics to assess the organization's security posture and Incident Readiness.

Success Rate of Adversarial Tactics

- Measure the success rate of adversarial tactics, techniques, and procedures (TTPs) employed by the red team during the engagement.

Time to Detection and Response

- Evaluate the time it took for the blue team to detect and respond to simulated attacks during the engagement.

Detection Coverage and False Positive Rate

- Assess the coverage of detection mechanisms deployed by the blue team, including intrusion detection systems (IDS), security information and event management (SIEM) solutions, and endpoint detection and response (EDR) tools.

Impact on Business Operations

- Evaluate the impact of simulated attacks on critical business operations, including downtime, data loss, financial losses, and reputational damage.

Effectiveness of Incident Response

- Measure the effectiveness of the organization's incident response procedures in mitigating and containing simulated cyber incidents. Evaluate key metrics such as containment time, eradication time, and recovery time to assess the efficiency and thoroughness of incident response efforts.

Security Awareness and Training

- Evaluate the effectiveness of security awareness and training programs in preparing employees to recognize and respond to simulated cyber threats.

Reporting

[redacted]

IR CARE Report
Wednesday, July 19, 2023

NETWITNESS
Netwitness Red Team

An RSA Business

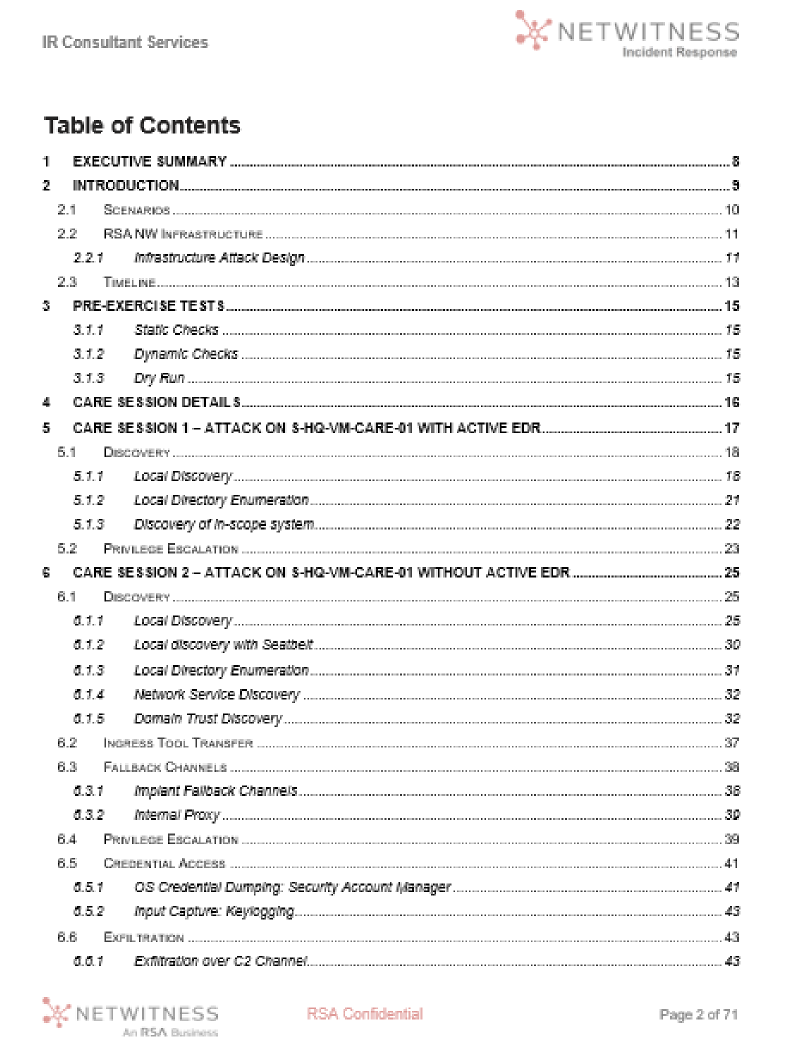
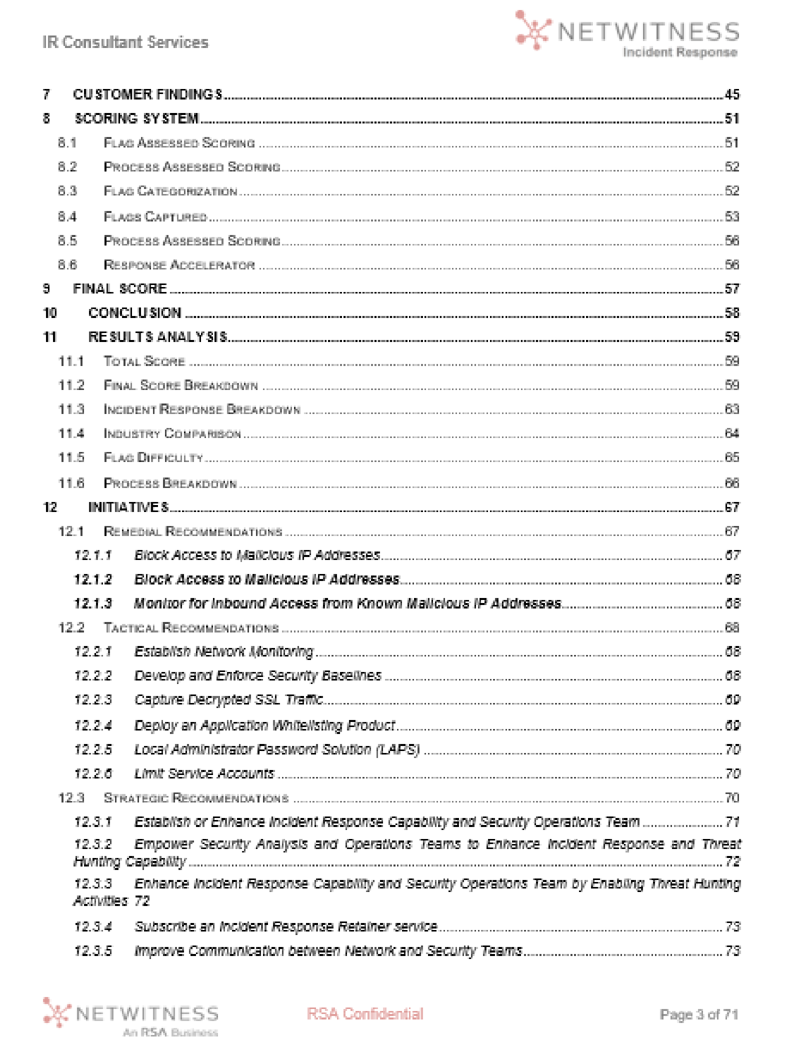


Table of Contents



Reporting

Time to Detection (TTD)

- Measure the time it took for the blue team to detect simulated attacks initiated by the red team.
- A shorter time to detection indicates a higher level of incident readiness, as it demonstrates the organization's ability to identify and respond promptly to security incidents.

Mean Time to Detect (MTTD)

- Calculate the average time it takes for the blue team to detect simulated attacks across multiple scenarios.
- A lower MTTD suggests more efficient detection mechanisms and a higher level of incident readiness.

Detection Coverage

- Evaluate the coverage of detection mechanisms deployed by the blue team, including intrusion detection systems (IDS), security information and event management (SIEM) solutions, and endpoint detection and response (EDR) tools.

Time to Response (TTR)

- Evaluate the time it took for the blue team to respond to simulated attacks once detected.
- Measure key response metrics, such as mean time to respond (MTTR) and mean time to contain (MTTC), to assess the efficiency and effectiveness of incident response efforts.

Incident Handling Procedures

- Assess the organization's incident handling procedures and protocols based on observations and findings from the red teaming test.
- Evaluate the clarity, completeness, and effectiveness of incident response playbooks, escalation procedures, and communication protocols.

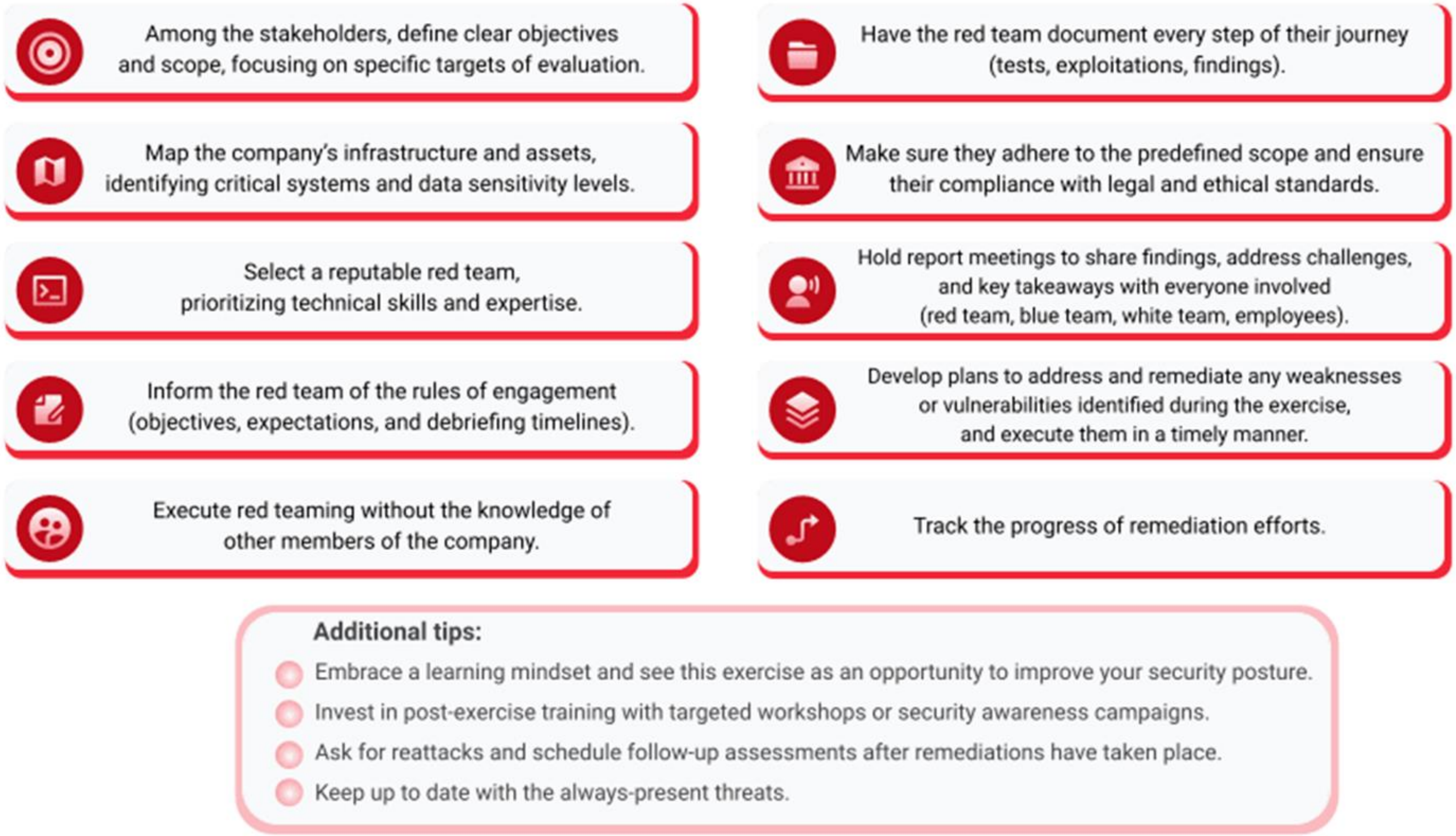
Resource Allocation and Coordination

- Evaluate the allocation of resources and coordination among different teams involved in incident response, including the blue team, IT operations, security operations center (SOC), legal, and executive management.
- Assess the effectiveness of collaboration and communication channels during the red teaming test.

Lessons Learned and Remediation Actions:

- Capture lessons learned from the red teaming test and identify actionable remediation actions to address gaps and weaknesses in incident readiness.

Conclusions: Checklist for a successful test



- Among the stakeholders, define clear objectives and scope, focusing on specific targets of evaluation.
- Map the company's infrastructure and assets, identifying critical systems and data sensitivity levels.
- Select a reputable red team, prioritizing technical skills and expertise.
- Inform the red team of the rules of engagement (objectives, expectations, and debriefing timelines).
- Execute red teaming without the knowledge of other members of the company.
- Have the red team document every step of their journey (tests, exploitations, findings).
- Make sure they adhere to the predefined scope and ensure their compliance with legal and ethical standards.
- Hold report meetings to share findings, address challenges, and key takeaways with everyone involved (red team, blue team, white team, employees).
- Develop plans to address and remediate any weaknesses or vulnerabilities identified during the exercise, and execute them in a timely manner.
- Track the progress of remediation efforts.

Additional tips:

- Embrace a learning mindset and see this exercise as an opportunity to improve your security posture.
- Invest in post-exercise training with targeted workshops or security awareness campaigns.
- Ask for reattacks and schedule follow-up assessments after remediations have taken place.
- Keep up to date with the always-present threats.

Thanks!