

Census Labs S.A.

Thinking Like an Adversary

Practical Introduction to Red Teaming



Ioannis Stais

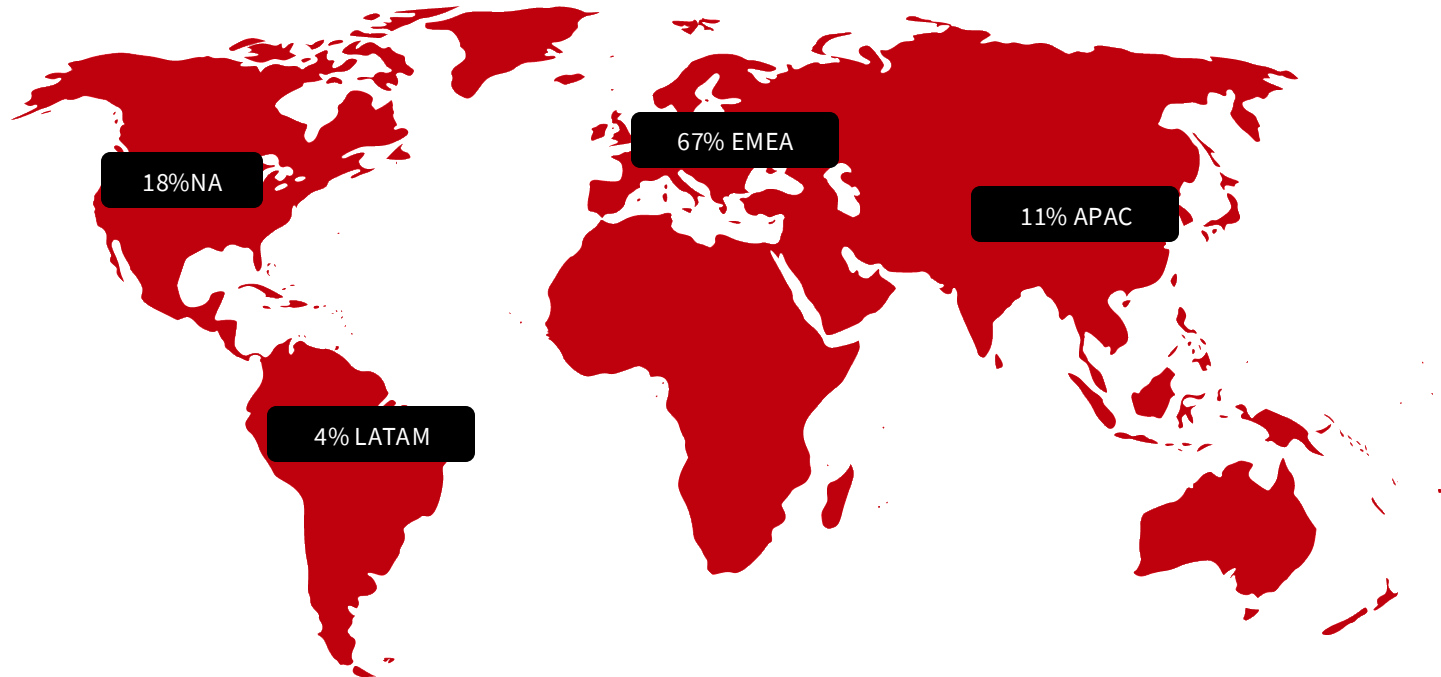
Director of Organization Security Testing
(istais@census-labs.com)



CENSUS at a glance

Global presence

We help clients with their **cybersecurity maturity journey** by providing **end to end** state of the art **assessment of their security posture** to improve their **cyber resilience** and leverage the benefits of **digital transformation**.



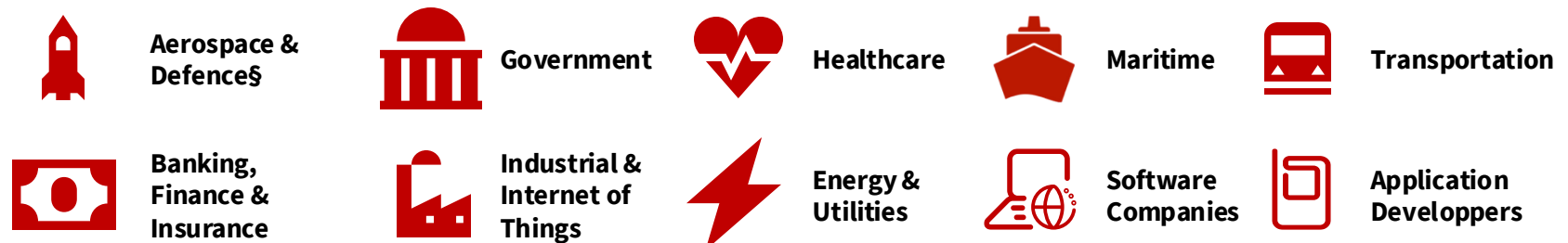
19+

Countries

~400

Clients
80+ Fortune 500

In multiple market sectors



CENSUS at a glance

- ◆ **CENSUS** is an **internationally acclaimed** Cybersecurity services provider, supporting the needs of **multiple industries**.
- ◆ We are offering state-of-the-art services to organizations **worldwide** to cover the complex needs of today's **IT & OT ecosystems**:
 - ◆ Security Assessments
 - ◆ Product Security
 - ◆ Secure Systems Development Lifecycle
 - ◆ Vulnerability Research
 - ◆ Information Security Consulting
- ◆ Services built upon the **company's leading research** to provide high quality InfoSec services.
- ◆ We are very proud of our **ethos**, as we care about **quality (in) systems**.

70+ Security engineers **12+** Years of innovation

Company certified for quality and security management systems



Thinking Like an Adversary: A Practical Introduction to Red Teaming

Agenda

- ◆ Red Teaming: Scope, Objectives, Goals, TTPs
- ◆ Threat Intelligence
- ◆ RT Methodology & Planning
- ◆ Reconnaissance
- ◆ Weaponization, Exploitation & Initial Access
- ◆ Privilege Escalation, Lateral Movement & Persistency
- ◆ Reporting & Debrief
- ◆ Ethical & Legal Consideration



Red Teaming: Scope, Objectives, Goals, TTPs



Red Teaming: Emulate real-world adversaries to test technology, people and processes

- ◆ **Full-scope, intelligence-led, multi-layered attack simulation** designed to measure how well a company's people and networks, applications processes and physical security controls can withstand an attack from a real-life adversary. The test will expose vulnerabilities and risks regarding:
 - ◆ Technology — Networks, applications, services, routers, switches, IoT appliances, access controls, etc.
 - ◆ People — Staff, independent contractors, interns, departments, business partners, etc.
 - ◆ Processes — IR playbooks, recovery, etc.
- ◆ Often operate over an extended time and combine multi-faceted testing approaches that are designed to not only seek to penetrate an organization but verify the detection, monitoring and incident response process and actions
- ◆ Aimed at improving resilience: It's a controlled simulation with rules and measurable objectives



Red Team vs Blue Team vs Purple Team vs ...

Type	Main Goal	Focus Areas	Typical Activities	Outcome / Value
Red Team (RT)	Realistic simulation of Threat Actors	Offensive real TTPs, covert operations, broad scope, persistence, focused on critical assets	Recon, Phishing, lateral movement, C2	Tests detection & response, reveals true gaps
Blue Team (BT)	Defend, Detect, Recover	Monitoring, IR, forensics	Log analysis, EDR, SIEM tuning, hunts	Detects attacks, contains & recovers incidents
Purple Team (PT)	Collaborate & improve	Red + Blue integration	Replay attacks, evaluate and refine controls	Faster detection, knowledge sharing, tuned defences
Gold Team (GT)	Govern & align	Strategy, risk, policy	Table-Top exercises, Ransomware	Assurance, governance, continuous improvement
Penetration Testing (PT)	Finds technical flaws	Vulnerability identification & exploitation, limited actions	Mapping / Scan, exploiting, reporting	Lists and validates security weaknesses



Red Team vs Blue Team vs Purple Team vs ...

Red Team

- You're the attacker!

Blue team

- You defend and escalate!

Purple Team

- You bridge both and coach!

Gold Team

- You oversee rules, playbooks and sign-offs!

Penetration Tester

- You conduct a focused technical assessment!





Goals & Objectives: Measure the organization's ability to detect, respond, and recover

- ◆ Identify security vulnerabilities across systems, processes and human behaviour
- ◆ Evaluate detection and response capability under realistic attack scenarios.
- ◆ Identify process and control failures (gaps in coverage, inefficient playbooks, errors in escalation, communication, etc).
- ◆ Test the organization's most critical assets and functions (crown jewels) under attack.
- ◆ Provide strategic insights: Deliver risk-based findings. Provide actionable intelligence about the organization's security posture.
- ◆ Drive blue team improvements

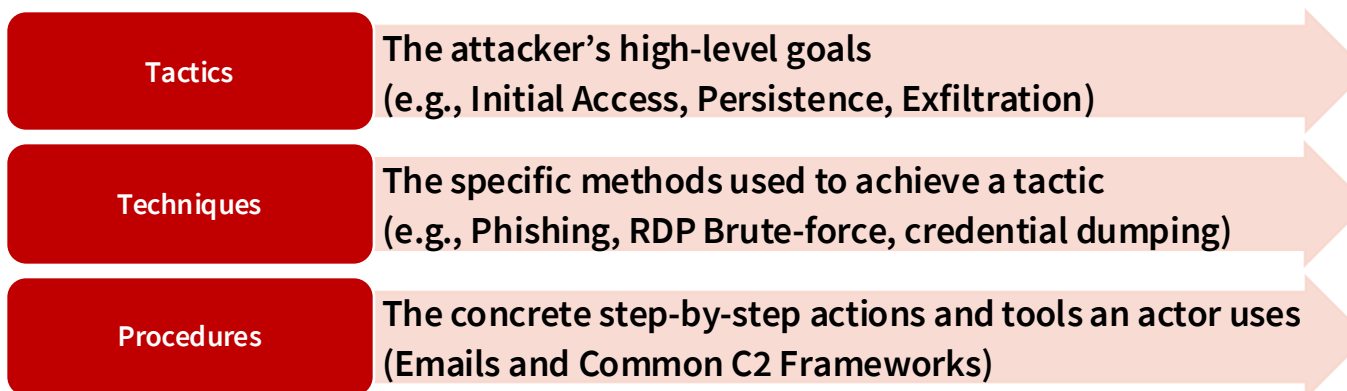
We should ensure that the simulation
accurately reflects authentic
cyber threat activity



The simulation should include real-world adversarial behaviours and TTPs

- ◆ **Threat Actor:** A person or a group of people that take part in malicious acts against systems, networks, or organizations
- ◆ **Motivation:** Can include financial gain, espionage, activism, political influence, or disruption.
- ◆ **Archetypes / Categories:** Nation-State Actors, Cybercriminals, Hacktivists, Insiders, Script Kiddies

Threat Actor TTPs:





INTEL TAL: A standardized Threat Agent archetypes knowledge base

	Intent	NON-HOSTILE			HOSTILE																	
		Employee Reckless	Employee Untrained	Info Partner	Anarchist	Civil Activist	Competitor	Corrupt Government Official	Data Miner	Employee Disgruntled	Government Cyberwarrior	Government Spy	Internal Spy	Irrational Individual	Legal Adversary	Mobster	Radical Activist	Sensationalist	Terrorist	Thief	Vandal	Vendor
Access (1)	Internal																					
	External																					
Outcome (1-2)	Acquisition/Theft																					
	Business Advantage																					
	Damage																					
	Embarrassment																					
Limits (max)	Tech Advantage																					
	Code of Conduct																					
	Legal																					
	Extra-legal, minor																					
Resources (max)	Extra-legal, major																					
	Individual																					
	Club																					
	Contest																					
Skills (max)	Team																					
	Organization																					
	Government																					
	None																					
Objective (1 or more)	Minimal																					
	Operational																					
	Adept																					
	Copy																					
Visibility (min)	Deny																					
	Destroy																					
	Damage																					
	Take																					
Multiple/Don't Care	All of the Above/ Don't Care																					
	Overt																					
	Covert																					
	Clandestine																					

Source: Intel IT Threat Assessment Group, 2007

URL: [https://https://www.researchgate.net/publication/324091298_Threat_Agent_Library_Helps_Identify_Information_Security_Risks](https://www.researchgate.net/publication/324091298_Threat_Agent_Library_Helps_Identify_Information_Security_Risks)



MITRE ATT&CK®: A TTP knowledge base based on real-world observations.

ATT&CK Matrix for Enterprise													
layout: side • show sub-techniques hide sub-techniques													
Reconnaissance 11 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 17 techniques	Persistence 22 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (2) Gather Victim Host Information (4) Gather Victim Identity Information (1) Gather Victim Network Information (4) Gather Victim Org Information (4) Phishing for Information (4) Search Closed Sources (2) Search Open Technical Databases (3) Search Open Websites/Domains (1) Search Threat Vendor Data Search Victim-Owned Websites	Acquire Access Acquire Infrastructure (8) Compromise Accounts (2) Compromise Infrastructure (4) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (2) Stage Capabilities (4) Supply Chain Compromise (1) Trusted Relationship Valid Accounts (4) Wi-Fi Networks	Content Injection Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (4) Replication Through Removable Media Supply Chain Compromise (1) Trusted Relationship Valid Accounts (4) Wi-Fi Networks	Cloud Administration Command Command and Scripting Interpreter (13) Container Administration Command Deploy Container ESX Administration Command Exploitation for Client Execution Input Injection Inter-Process Communication (2) Native API Poisoned Pipeline Execution Scheduled Task/Job (2) Serverless Execution Shared Modules Software Deployment Tools System Services (2) User Execution (2) Windows Management Instrumentation	Account Manipulation (2) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Cloud Application Integration Compromise Host Software Binary Create Account (2) Create or Modify System Process (2) Event Triggered Execution (13) Exclusive Control External Remote Services Hijack Execution Flow (2) Implant Internal Image Modify Authentication Process (1) Modify Registry Office Application Startup (4) Power Settings Pre-OS Boot (4) Scheduled Task/Job (2) Server Software Component (4) Software Extensions (2) Traffic Signaling (2) Valid Accounts (4)	Abuse Elevation Control Mechanism (1) Access Token Manipulation (2) BITS Jobs Build Image on Host Debugger Evasion Delay Execution Deadfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain or Tenant Policy Modification (2) Email Spoofing Execution Guardrails (2) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (14) Hijack Execution Flow (2) Impair Defenses (2) Impersonation Indicator Removal (13) Indirect Command Execution Masquerading (12) Modify Authentication Process (4) Modify Cloud Compute Infrastructure (3) Modify Cloud Resource Hierarchy Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (17) Pilot File Modification	Abuse Elevation Control Mechanism (1) Access Token Manipulation (2) BITS Jobs Build Image on Host Debugger Evasion Delay Execution Deadfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain or Tenant Policy Modification (2) Email Spoofing Execution Guardrails (2) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (14) Hijack Execution Flow (2) Impair Defenses (2) Impersonation Indicator Removal (13) Indirect Command Execution Masquerading (12) Modify Authentication Process (4) Modify Cloud Compute Infrastructure (3) Modify Cloud Resource Hierarchy Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (17) Pilot File Modification	Adversary-in-the-Middle (4) Brute Force (4) Credentials from Password Stores (3) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (4) Multi-Factor Authentication Interception OS Credential Dumping (4) Steal Application Access Token Steal or Forge Authentication Certificates Steal or Forge Kerberos Tickets (4) Steal Web Session Cookie Unsecured Credentials (8)	Account Discovery (4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Device Driver Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Local Storage Discovery Log Enumeration Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (2) Process Discovery Query Registry Remote System Discovery Software Discovery (2) System Information Discovery System Location Discovery (1) System Network Configuration Discovery (2) System Network Connections Discovery System Parameter Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (4) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (4) Archive Collected Data (2) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (1) Data from Information Repositories (4) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (4) Input Capture (4) Screen Capture Video Capture	Application Layer Protocol (4) Communication Through Removable Media Content Injection Data Encoding (2) Data Obfuscation (2) Dynamic Resolution (2) Encrypted Channel (2) Fallback Channels Hide Infrastructure Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Tools (2) Traffic Signaling (2) Web Service (2)	Automated Exfiltration (2) Data Transfer Size Limits Exfiltration Over Alternative Protocol (1) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (4) Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction (1) Data Encrypted for Impact Data Manipulation (3) Defacement (2) Disk Wipe (2) Email Bombing Endpoint Denial of Service (4) Financial Theft Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking (4) Service Stop System Shutdown/Reboot

URL: <https://attack.mitre.org>

We must take into account industry-specific threat levels

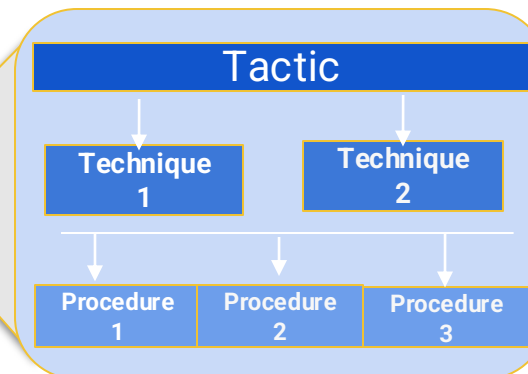
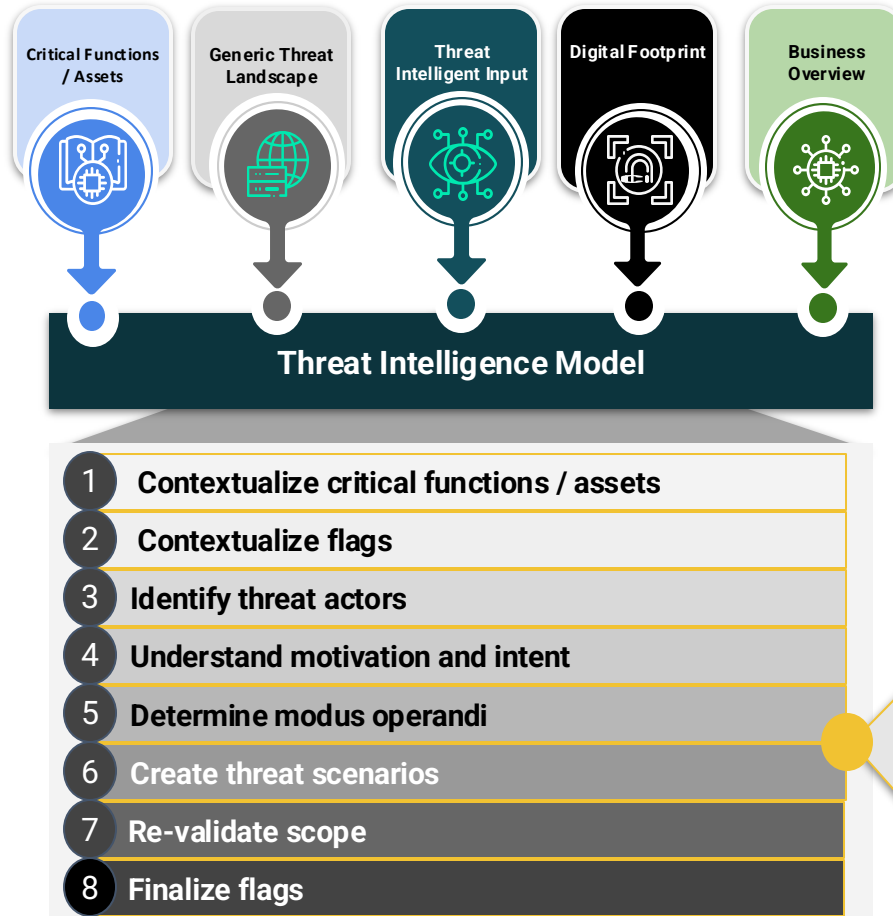
Tailored to a security organization's unique attack surface



Threat Intelligence



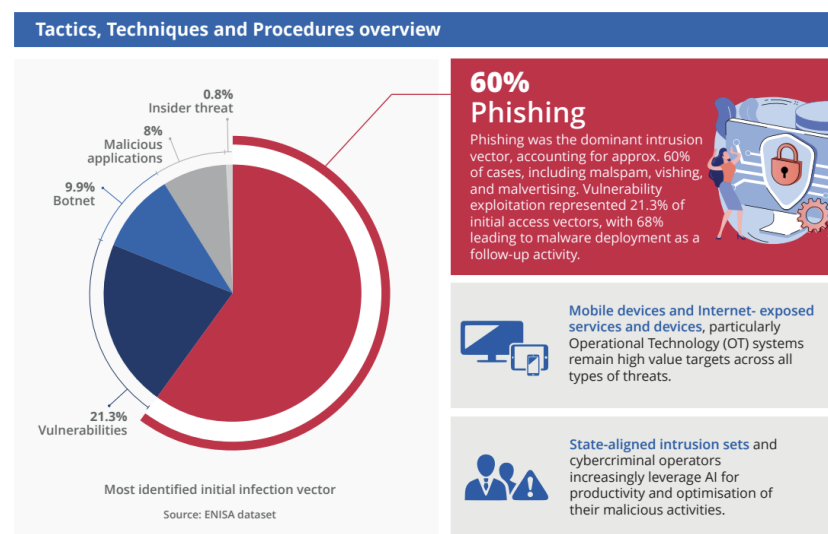
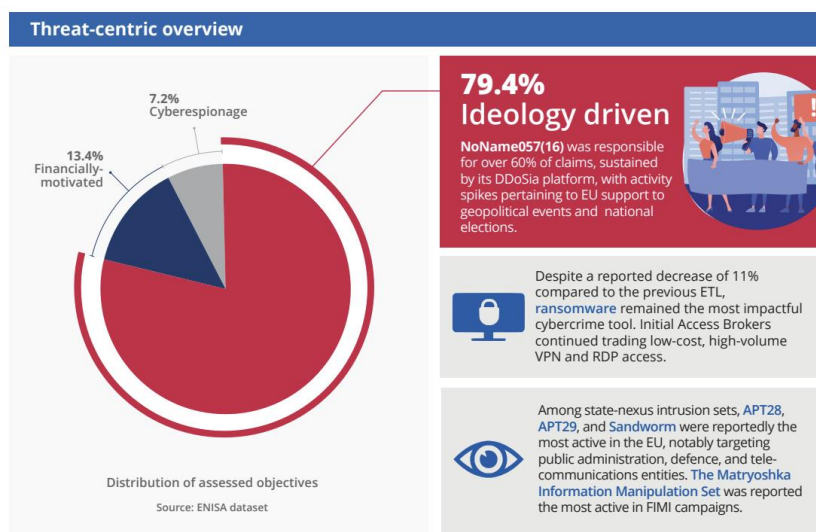
Phases of Threat Intelligence





ENISA Generic Threat Landscape 2025

- ◆ ENISA Threat Landscape analyses 4875 incidents over a period spanning from 1 July 2024 to 30 June 2025.
- ◆ This report provides an overview of the most prominent cybersecurity threats and trends the EU faces



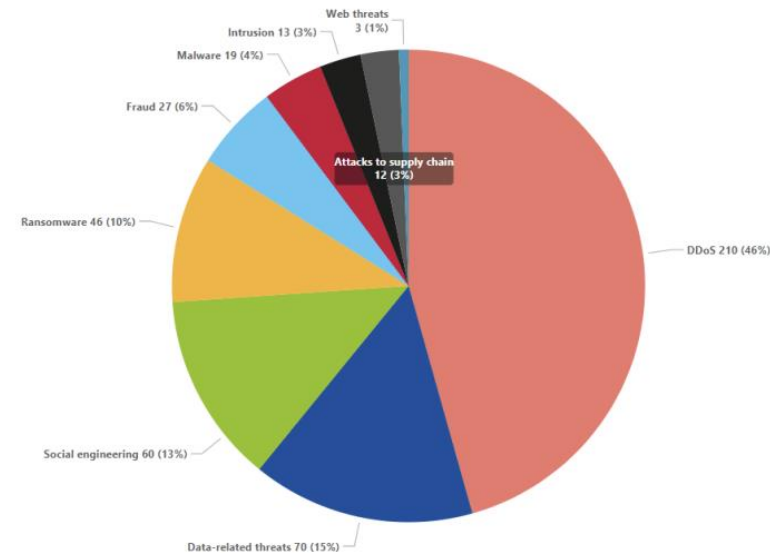


ENISA Threat Landscape – Financial Sector

- ◆ From January 2023 to June 2024, the European financial sector faced significant cybersecurity challenges, highlighting threats and vulnerabilities across the sector.



Figure 5: Threats observed in the European finance sector (January 2023 to June 2024)



URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector>



MITRE ATT&CK Groups / Threat Actor Catalog

- ◆ Groups are activity clusters that are tracked by a common name in the security community. MITRE ATT&CK tracks more than 160 such groups

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy , as well as some non-public backdoors.
G1030	Agrius	Pink Sandstorm, AMERICIUM, Agonizing Serpens, BlackShadow	Agrius is an Iranian threat actor active since 2020 notable for a series of ransomware and wiper operations in the Middle East, with an emphasis on Israeli targets. Public reporting has linked Agrius to Iran's Ministry of Intelligence and Security (MOIS).
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.
G1024	Akira	GOLD SAHARA, PUNK SPIDER, Howling Scorpis	Akira is a ransomware variant and ransomware deployment entity active since at least March 2023. Akira uses compromised credentials to access single-factor external access mechanisms such as VPNs for initial access, then various publicly-available tools and techniques for lateral movement....

URL: <https://attack.mitre.org/groups/>



Collecting Information From Multiple Sources

- ◆ Open-source (OSINT), commercial feeds, dark web, sensors, telegram and internal logs.

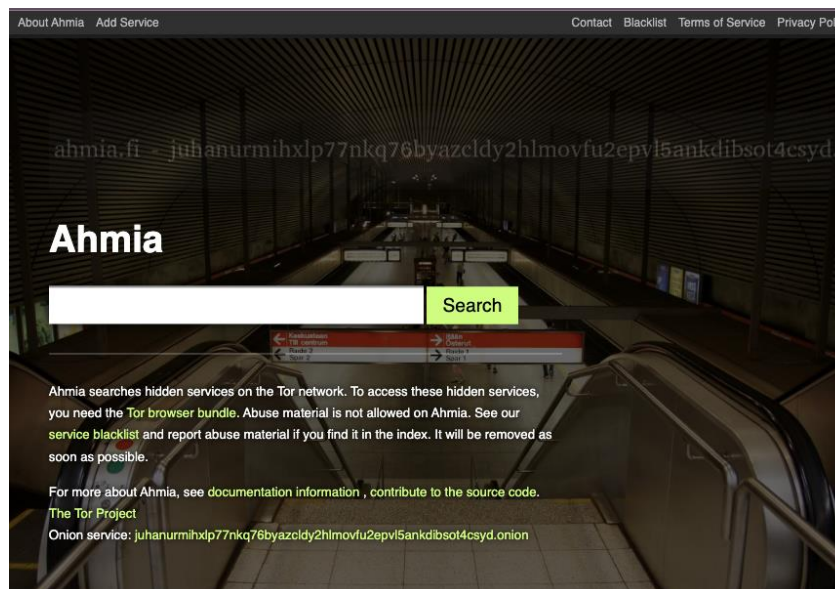
```
root@kali:~# theHarvester -d kali.org -l 500 -b duckduckgo
*****
* theHarvester 4.4.3
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: kali.org
[*] Searching Duckduckgo.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 14
[...]
'''console
```

URL: <https://github.com/laramies/theHarvester>



URL: <https://github.com/DedSecInside/TorBot>



URL: <https://ahmia.fi/>

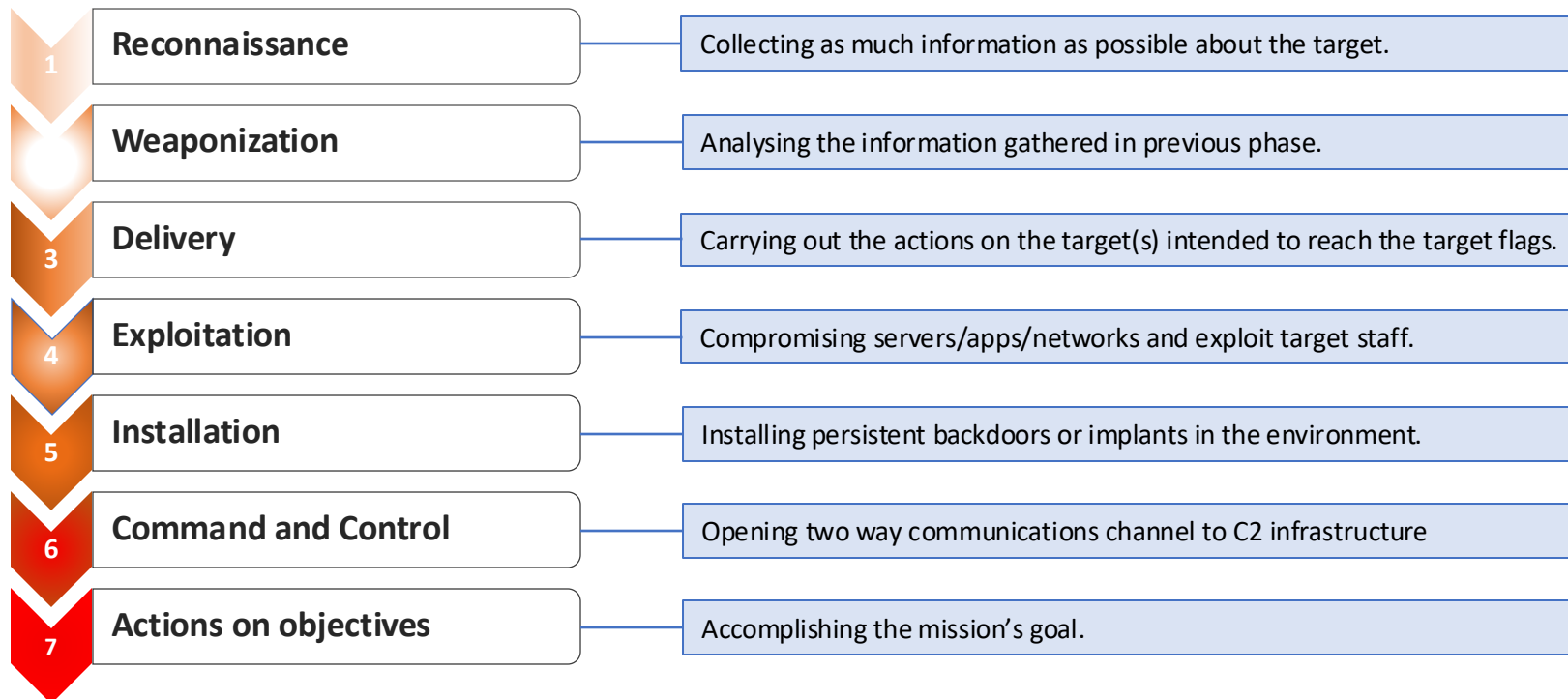


Methodology



Testing phase | Red Team Testing Methodology

- ◆ The testing methodology is primarily based on the Cyber Kill Chain (CKC) of the Intelligence Driven Defense model for identification and prevention of cyber intrusions activity, developed by Lockheed Martin

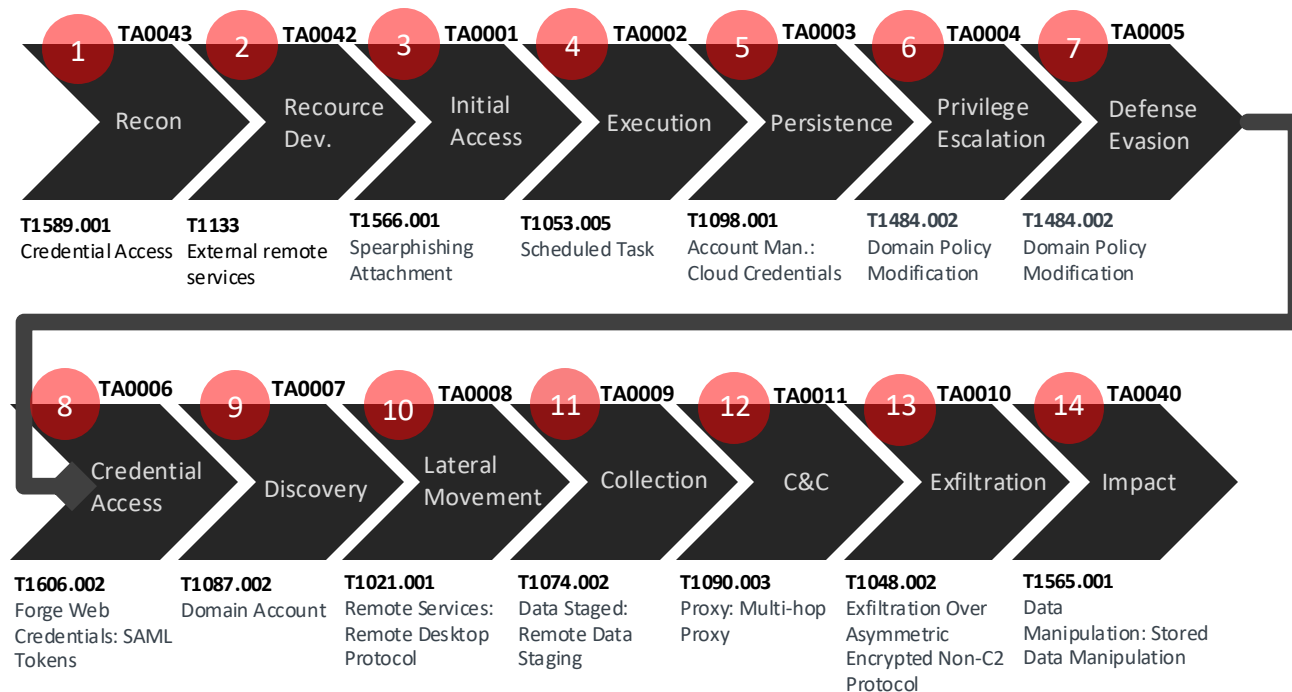




Testing phase | Red Team Testing Methodology

MITRE ATT&CK Enterprise tactics

- ◆ ATT&CK is used as a lower level of definition to map the actions as an adversary.
- ◆ Example of mapping TTPs of **APT29** to the ATT&CK.





Testing phase | Red Team Testing Methodology

Other widely accepted methodologies

- ◆ OWASP Testing Guide
- ◆ OWASP Application Security Verification Standard,
- ◆ NIST Technical Guide to Information Security Testing and Assessment
- ◆ PTES standard
- ◆ Open-Source Security Testing Methodology Manual





Planning & Scoping

- ◆ Define allowed targets, prohibited techniques, and data handling rules.
- ◆ Set success criteria and acceptable business impact (e.g., no production outages).
- ◆ Decide communication cadence, **emergency kill-switch**, and **escalation contacts**.
- ◆ **Capture legal approvals** and executive sponsorship in writing.
- ◆ Build a controlled test plan with risk mitigations (backups, rollback).



Reconnaissance



Reconnaissance

◆ Internet Fingerprinting & Passive Reconnaissance involves:

- ◆ **Web Search:** A comprehensive search approach to gather a diverse range of data, including important contact details, addresses, up-to-date news, articles, social media content, leaked credentials, exploration of an organization's digital footprint on websites, blogs, social media profiles, online discussions, and other relevant online presence indicators.
- ◆ **Business Registry Search:** Reveals several details regarding a company's history, organization, and operations.
- ◆ **Whois and RIRs:** Querying databases holding information of registered users or assignees of Internet.
- ◆ **Autonomous System Number (ASN) Lookup:** Identification of the Autonomous System (AS) number associated with a specific IP address.

Αναζήτηση στην Δημοσιότητα ΓΕΜΗ

CENSUS ΑΝΩΝΥΜΗ ΕΤΑΙΡΙΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ	
Αριθμός ΓΕΜΗ	043476106000
EUID	ELGEM.043476106000
Διακριτικοί Τίτλοι	CENSUS A.E.
Επωνυμία με λατινικούς χαρακτήρες	(Δεν βρέθηκε κάποιο στοιχείο)
AΦΜ	998387604
Ημ/νία Σύστασης	31/03/2008
Νομική Μορφή	ΑΕ
Κατάσταση	Ενεργή από 31/03/2008
Διεύθυνση	ΙΔΑΝΝΟΥ ΓΚΟΥΡΑ 16, ΘΕΣΣΑΛΟΝΙΚΗΣ / ΘΕΣΣΑΛΟΝΙΚΗΣ, 54352
Ιστοσελίδα	www.census-labs.com/census/financial
e-shop	(Δεν βρέθηκε κάποιο στοιχείο)

RIPE Database

Enter a search term
google.com

Types ▾ Hierarchy flags ▾ Inverse lookup ▾ Advanced filter ▾

By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

Earn the RIPE Database Associate certification
Do you use the RIPE Database regularly as a researching and data register Database.
[Find out more](#) about how you can earn the RIPE Database Associate badge

Search results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is a free service.

inet-rtr:	Google.com
org:	ORG-NA1296-RIPE
local-as:	As197287
ifaddr:	172.217.169.238 Masklen 0
ifaddr:	172.217.0.0 Masklen 0
admin-c:	AA37671-RIPE
tech-c:	AA37671-RIPE
mnt-by:	Jb71-mnt
created:	2021-06-10T15:02:02Z
last-modified:	2021-06-10T15:14:15Z
source:	RIPE

RIPE Database Software Version 1.107



Reconnaissance

◆ Internet Fingerprinting & Passive Reconnaissance involves:

- ◆ **Domain Name System Enumeration:** Gathering information about DNS servers, DNS records, and the types of servers in-use.
- ◆ **Certificate Transparency:** Identification of subdomains using the publicly available CT Logs.
- ◆ **Subdomain Automated Dictionary Attacks:** Trying systematically to identify valid subdomains using a dictionary or list of potential subdomain names.
- ◆ **Email Gathering:** Collecting emails from target companies or individuals that are publicly available.

cr

tl

id

Identity

Search

Group by: Issuer

Criteria

Type: Identity

Match: ILIKE

Search: 'census-labs.com'

Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
2023-08-18	2023-08-18	2023-11-16	census-labs.com	*census-labs.com www.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-08-07	2023-08-07	2023-11-05	census-labs.com	*census-labs.com www.census-labs.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
2023-08-07	2023-08-07	2023-11-05	census-labs.com	*census-labs.com www.census-labs.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
2023-07-25	2023-07-25	2023-10-23	test.census-labs.com	*census-labs.com test.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-07-23	2023-07-23	2023-10-21	files.census-labs.com	*census-labs.com files.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-06-27	2023-06-27	2023-09-25	woas.census-labs.com	*census-labs.com woas.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-06-27	2023-06-27	2023-09-25	woas.census-labs.com	*census-labs.com woas.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-06-26	2023-06-26	2024-07-24	woas.census-labs.com	*census-labs.com woas.census-labs.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
2023-06-26	2023-06-26	2024-07-24	woas.census-labs.com	*census-labs.com woas.census-labs.com	C=US, O=Amazon, CN=Amazon RSA 2048 M01
2023-06-26	2023-06-26	2024-07-24	woas.census-labs.com	*census-labs.com woas.census-labs.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
2023-06-19	2023-06-19	2023-09-17	report.census-labs.com	*census-labs.com report.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-06-19	2023-06-19	2023-09-17	report.census-labs.com	*census-labs.com report.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-06-19	2023-06-19	2023-09-17	census-labs.com	*census-labs.com www.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-06-16	2023-06-16	2023-09-07	census-labs.com	*census-labs.com census-labs.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
2023-06-09	2023-06-09	2023-09-07	census-labs.com	*census-labs.com census-labs.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
2023-06-02	2023-06-02	2024-06-10	castor.census-labs.com	*census-labs.com castor.census-labs.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Thawte TLS RSA CA G1
2023-06-02	2023-06-02	2024-06-10	pollux.census-labs.com	*census-labs.com pollux.census-labs.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Thawte TLS RSA CA G1
2023-05-26	2023-05-26	2023-08-24	test.census-labs.com	*census-labs.com test.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-05-24	2023-05-24	2023-08-22	files.census-labs.com	*census-labs.com files.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-04-19	2023-04-19	2023-07-18	report.census-labs.com	*census-labs.com report.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-04-19	2023-04-19	2023-07-18	report.census-labs.com	*census-labs.com report.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-04-19	2023-04-19	2023-07-18	census-labs.com	*census-labs.com www.census-labs.com	C=US, O=Let's Encrypt, CN=R3
2023-04-14	2023-04-11	2023-07-10	*census-labs.com	*census-labs.com www.census-labs.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
2023-04-11	2023-04-11	2023-07-10	*census-labs.com	*census-labs.com census-labs.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
2023-04-01	2023-02-11	2023-05-12	*census-labs.com	*census-labs.com census-labs.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5

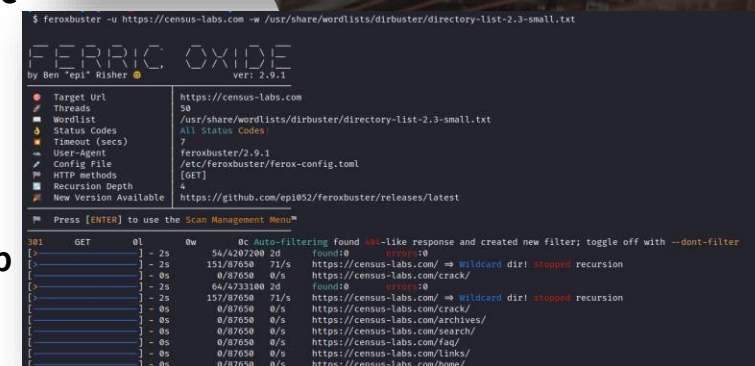
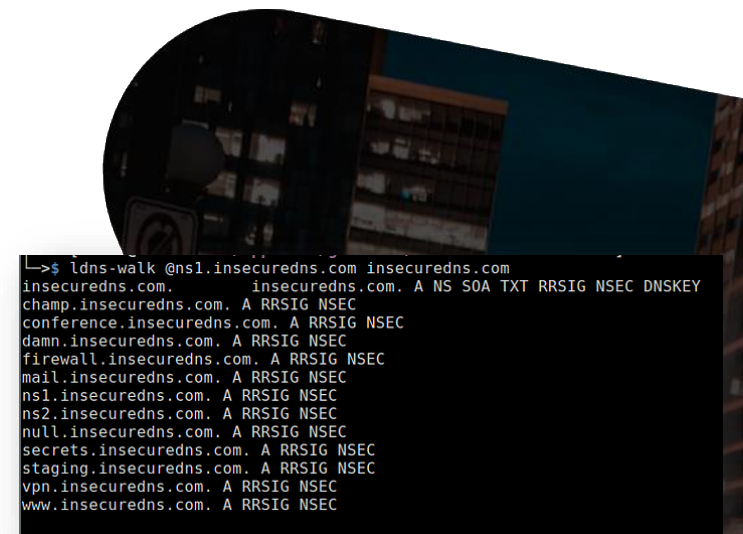
DNS Servers		
lily.ns.cloudflare.com.	173.245.58.130	CLOUDFLARENET
lily.ns.cloudflare.com.	lily.ns.cloudflare.com	United States
miguel.ns.cloudflare.com.	172.64.35.95	CLOUDFLARENET
miguel.ns.cloudflare.com.	miguel.ns.cloudflare.com	United States
MX Records ** This is where email for the domain goes...		
0 censuslabs-com01e.mail.protection.outlook.com.	52.101.73.12	MICROSOFT-CORP-MSN-AS-BLOCK
mail-am4pr0401cu00104.inbound.protection.outlook.com		Netherlands
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
mail1.census-labs.com	195.97.34.23	HOI-GR Athens, Greece
mail1.census-labs.com	mail1.census-labs.com	Greece
mail2.census-labs.com	62.103.39.146	OTENET-GR Athens - Greece
mail2.census-labs.com	mail2.census-labs.com	Greece
mail3.census-labs.com	188.117.216.226	HCN-01 *** Peering Info from HCN ***
mail3.census-labs.com	mail3.census-labs.com	Upstream Austria



Reconnaissance

◆ Active Reconnaissance involves:

- ◆ **DNS Zone Walking:** walking in DNSSEC zones to enumerate all content. DNSSEC's NSEC/NSEC3 records provide information about the range of existing domain names, even if some of these names are not published or visible through normal DNS queries.
- ◆ **Network Port Scanning:** Sending network requests to different ports on a target system to determine which ports are open and listening for connections (TCP Connect, SYN/Stealth, UDP)
- ◆ **Service Version Identification:** Determine software versions to identify known vulnerabilities
- ◆ **Web Folders Enumeration Attack:** Known as directory or path enumeration attack, involves systematically attempting to identify and access hidden or sensitive directories and folders on a web server.
- ◆ **Vulnerability Scanning:** An industry-standard automated vulnerability scanning tool is used to search for publicly reported security issues in third-party software and services' configurations.
- ◆ **Manual Inspection of Accessible Network Services:** The services are analyzed by the team.

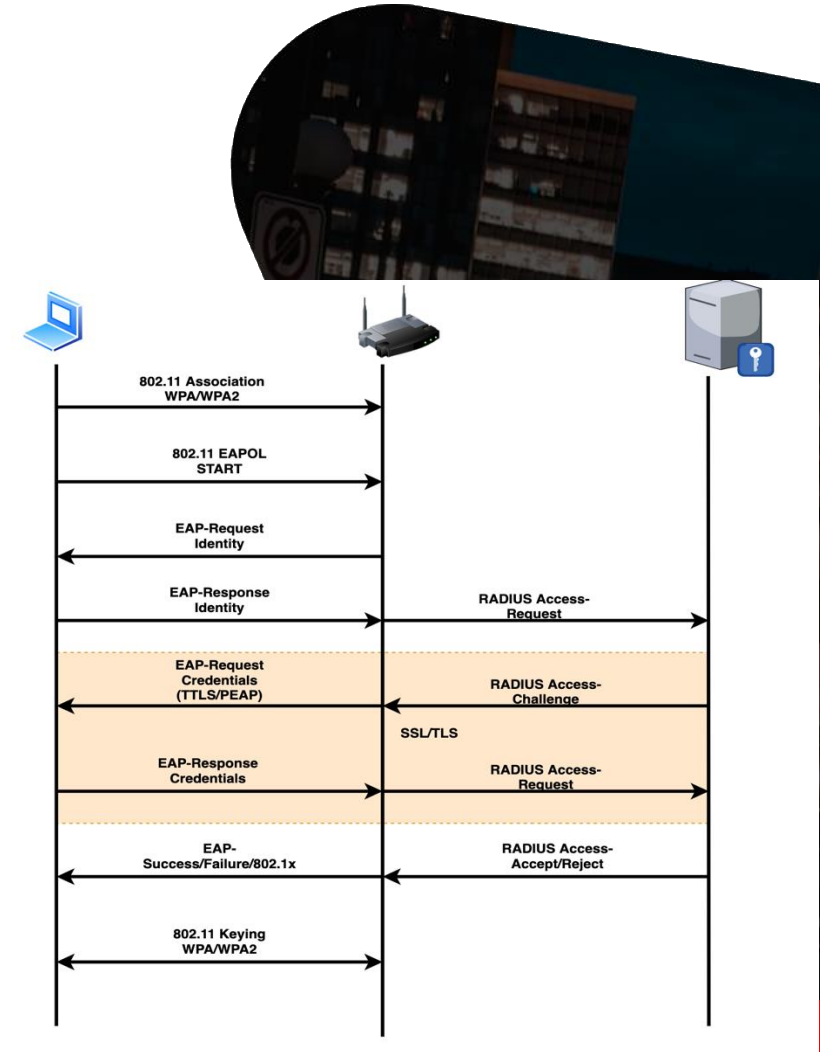




Reconnaissance

◆ Wireless Reconnaissance

- ◆ Passive Wi-Fi discovery: collect SSIDs, BSSIDs, channels, beacon frames, and signal strength.
- ◆ BT Client & device enumeration: observe probe requests, Bluetooth/LE advertisements, and device vendors
- ◆ Infrastructure inventory: map authorized APs, guest networks, IoT endpoints, and weak encryption settings.
- ◆ RF footprint mapping: wardrive or site sweep to record coverage gaps, signal bleed, and physical exposure.





Reconnaissance

◆ Physical Premises Reconnaissance

- ◆ Perimeter & entry points: gates, doors, loading docks, delivery entrances, shift change windows.
- ◆ Access control checks: badge readers, interlocks, visitor flows, tailgating opportunities, and signage.
- ◆ Points-of-Sale & kiosks: POS placement, unattended terminals, exposed USB/network ports
- ◆ Cameras & CCTV posture: camera locations, blind spots, camera cables
- ◆ Environmental & human factors: lighting, landscaping (hiding spots), employee routines, vendor deliveries, and contractor access.





Reconnaissance

◆ Sample Basic Tooling

- ◆ dirb - directory buster (wordlist-based web content discovery): <https://github.com/v0re/dirb>
- ◆ gobuster - fast directory/file, DNS and vhost brute-forcer (Go): <https://github.com/OJ/gobuster>
- ◆ theHarvester - OSINT collector for emails, subdomains, names: <https://github.com/laramies/theHarvester>
- ◆ BBOT - OSINT / subdomain enumeration: <https://github.com/blacklanternsecurity/bbot>
- ◆ dnsrecon - DNS enumeration: <https://github.com/darkoperator/dnsrecon>
- ◆ Gitleaks - find secrets in github repos: <https://github.com/gitleaks/gitleaks>
- ◆ Trufflehog - find secrets in github, s3, Jenkins, postman, elasticsearch, huggingface: <https://github.com/trufflesecurity/trufflehog>
- ◆ nmap - network mapper: <https://github.com/nmap/nmap>
- ◆ Aircrack-ng - suite for Wi-Fi monitoring and auditing (includes airodump-ng): <https://github.com/aircrack-ng/aircrack-ng>
- ◆ bettercap - wireless monitoring (Wi-Fi, BLE, HID, more): <https://github.com/bettercap/bettercap>
- ◆ Kismet - wardriving: <https://www.kismetwireless.net>





Weaponization, Exploitation, Initial Access



Weaponization, Exploitation, Initial Access

◆ **Weaponization and Delivery involves:**

- ◆ **Attack Planning:** Classification of the riskiest attack paths which have the easiest exploitation. The above classification helps in the understanding of the risks and also simulates the worst-case scenarios with respect to the vulnerabilities found. **TTPs that are requested for simulation are also taken into account.**
- ◆ **Vulnerability Research / Creating Custom Exploits:** The exploit could be a zero-day or a known vulnerability that the attacker expects will not have been patched.
- ◆ **Combining the payload with custom agent:** This can be anything that performs malicious actions, such as data exfiltration, system damage, or establishing a persistent presence for further exploitation.
- ◆ **Testing evasion techniques / IDS Bypass:** Ensuring that the weaponized content can bypass security measures like firewalls, intrusion detection systems, and antivirus software.
- ◆ **Transmission to the Target:** Sending the payload to the target directly over a network, such as through a vulnerable public-facing server.



Weaponization, Exploitation, Initial Access

◆ **Exploitation involves:**

- ◆ **Known vulnerability exploitation:** Exploiting known vulnerabilities in software and systems using tools like Metasploit. Attempting to exploit zero-day vulnerabilities or unpatched systems.
- ◆ **Password-based / Credential attacks:** Brute force attacks to guess passwords, Dictionary attacks with lists of commonly used passwords, Credential stuffing attacks
- ◆ **Web Services Attacks:** Abusing common OWASP Top-10 vulnerabilities (SQL injection, XSS, XSRF, LFI, etc.).
- ◆ **DNS Hijacking and Subdomain Takeover:** Redirecting traffic from a legitimate domain to a malicious one, Taking over unclaimed or improperly configured subdomains.
- ◆ **Memory-related Attacks:** Exploiting applications by overrunning a buffer's boundary
- ◆ **Exploiting Misconfigurations:** Taking advantage of insecure configurations in systems and applications, such as default credentials or open shares.
- ◆ **Session Hijacking, Token Manipulation Attacks:** Intercepting and using valid session tokens
- ◆ **Cloud Infrastructure Attacks:** Taking advantage of insecure configurations in cloud buckets





Initial Access

◆ Social Engineering attacks

- ◆ Collection of open-source intelligence information about employees (Victims identification, including high-profile targets - whaling)
- ◆ **Social engineering attacks such as Spear phishing, Baiting, Scareware, Pretexting & Client-side attacks.**
- ◆ **Typosquatting**
- ◆ **AI-driven social engineering attacks (e.g. Deepfake vishing, AI-generated spear phishing)**
- ◆ **Build customized payloads (malwares / trojans) that circumvent EDRs**
- ◆ **Pack initial access vectors for luring victims to execute the payloads (e.g. ISO, MSC, HTA)**
- ◆ **Social networks & Third Party Services Abuse for payload delivery**



URL:
<https://shop.hak5.org/products/omg-cable>

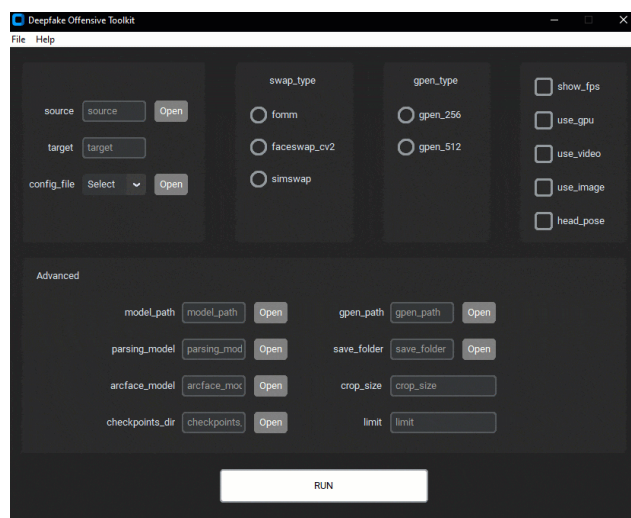


URL: <https://shop.hak5.org/products/usb-rubber-ducky>

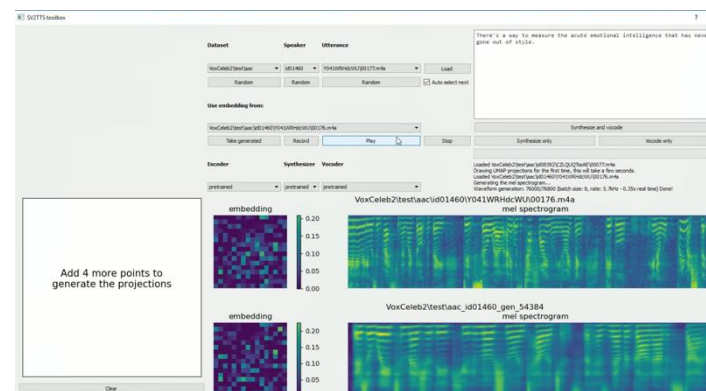


Initial Access

◆ Deepfake attacks



URL: <https://github.com/redteam-re/dot>



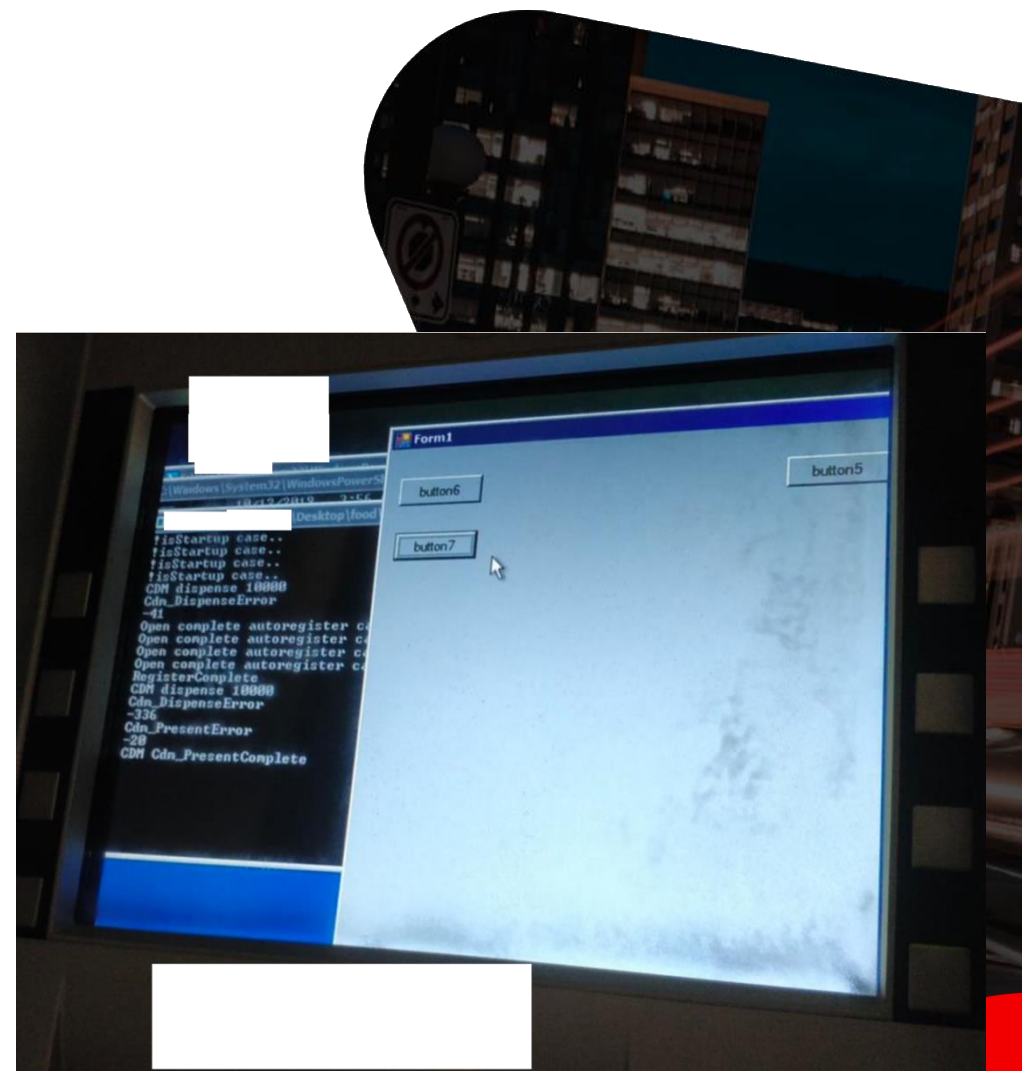
URL: <https://github.com/CorentinJ/Real-Time-Voice-Cloning>



Initial Access

◆ Physical Attacks

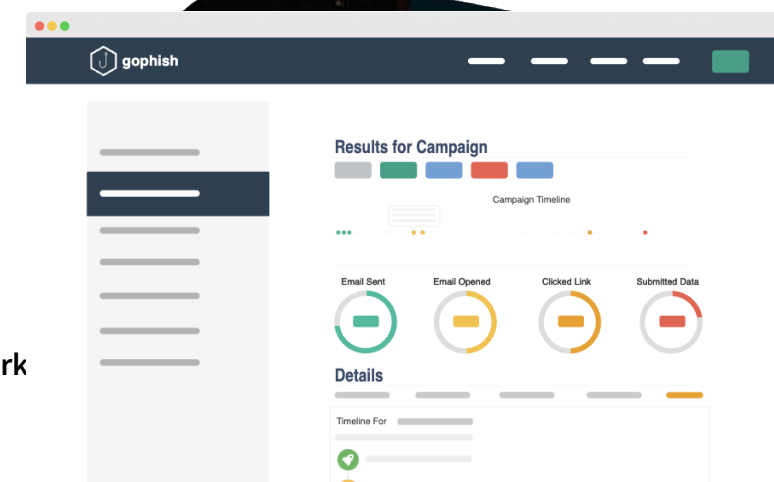
- ◆ Gaining physical access in premises: tailgating, stolen/unattended badges, insecure vendor access,
- ◆ Tampering with devices: unattended terminals / USB ports / PoS devices / IoT devices.
- ◆ Implanting devices (Evil Maid Attack): Gaining remote access in the network





◆ Sample Basic Tooling

- ◆ **sqlmap** - automated SQL injection discovery and exploitation: <https://github.com/sqlmapproject/sqlmap>
- ◆ **Metasploit Framework** - exploitation framework & payload generation: <https://github.com/rapid7/metasploit-framework>
- ◆ **Havoc** - post-exploitation / C2 agent framework: <https://github.com/HavocFramework/Havoc>
- ◆ **Sliver** - post-exploitation / C2 agent framework: <https://github.com/BishopFox/sliver>
- ◆ **Gophish** - phishing campaign platform: <https://github.com/gophish/gophish>
- ◆ **Phishing Frenzy** - phishing campaign platform: <https://github.com/pentestgeek/phishing-frenzy>
- ◆ **Evilginx** - browser man-in-the-middle attack: <https://github.com/kgretzky/evilginx2>
- ◆ **dnstwist** - typosquatting software: <https://github.com/elceef/dnstwist>
- ◆ **Social-Engineer Toolkit (SET)** - scenario builder (email templates, USB baiting simulations): <https://github.com/trustedsec/social-engineer-toolkit>
- ◆ **Red Baron** – Red Team Infrastructure Automation: <https://github.com/byt3bl33d3r/Red-Baron>

[illegible]

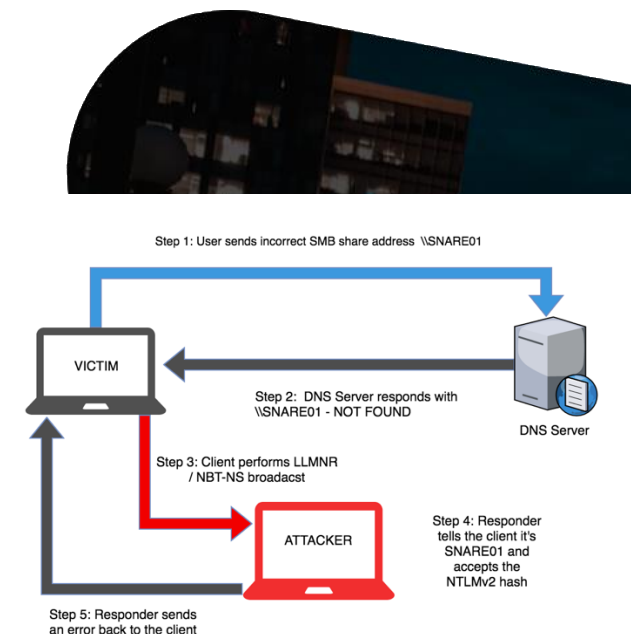


Privilege Escalation, Lateral Movement & Persistency



◆ Internal Network Reconnaissance & Priv. Escalation and Lateral Movement:

- ◆ **Network Shares Scanning:** If network shares are accessible, they may contain sensitive data
- ◆ **Domain Mapping:** The Active Directory is enumerated using tools such as Bloodhound.
- ◆ **Network Port Scanning:** Sending network requests to different ports on a target system to determine which ports are open and listening for connections (TCP Connect, SYN/Stealth, UDP)
- ◆ **Name Resolution Protocols Spoofing:** LLMNR/NBNS/mDNS - If such packets are travelling in the network, hijack them to obtain hashes for cracking.
- ◆ **Null Authentication Testing:** Attempting to authenticate against various services (like SMB, LDAP) for identification of open shares.
- ◆ **Password-based / Credential attacks:** Brute force attacks to guess passwords, Dictionary attacks with lists of commonly used passwords, Credential stuffing attacks using breached username and password pairs



Step 5: Responder sends an error back to the client

[illegible]



Privilege Escalation & Lateral Movement

◆ Active Directory specific attacks:

- ◆ **Kerberoasting:** Exploiting Kerberos TGS tickets for cracking.
- ◆ **ASREP Roasting:** Attacking users with non-pre-authentication requirement.
- ◆ **Insecure Delegation:** Abusing permissions forwarding within a domain.
- ◆ **Coercion and relay:** force a workstation to perform a connection, intercept and reuse the authentication sessions.
- ◆ **Cross-domain Trust Relationships:** Exploiting trust relationships between multiple domains.
- ◆ **GPO attacks:** Targeting insecure Group Policy configuration for privilege escalation.
- ◆ **Certificate Services:** Abusing insecure PKI services configuration for credentials theft/manipulation.

```
PS C:\Shared\Tools\Rubeus> .\Rubeus.exe kerberoast /format:hashcat

Rubeus
v1.6.4

[*] Action: Kerberoasting
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
    Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.
[*] Searching the current domain for Kerberoastable users
[*] Total kerberoastable users : 1

[*] SamAccountName      : SQLServiceAccount
[*] DistinguishedName    : CN=SQLServiceAccount,CN=Users,DC=rootdse,DC=lab
[*] ServicePrincipalName  : MSSQLSvc/sqlserver.rootdse.lab
[*] PwdLastSet            : 6/29/2021 5:48:46 PM
[*] Supported ETYPES     : RC4_HMAC_DEFAULT
[*] Hash                 : 84b58532255SQLServiceAccount$rootdse.lab$MSSQLSvc/sqlserver.rootdse.lab*$9D9C6
679EB4A5996ADE909F0025B348D5F5C08FFEAB36B795331DF8AF229C45C52385B2AC371007103808
67B723CA5EC83EA2D632E05EB051DDF06E7D52249F20E1C08FC9A0D19B44C4AE71DBFC221109EABD
1C90163D5FD54B31720F63779884D0A660CDA255ED198F20213B1CD99CD30661BE8F29DD246F1EB
99C0D94138C05E1B62DA2438A2DBEC120342C46923C10C49C34C49C5508B90E9605F9070C92C5
9D64FF6E105A50AAA1ABA6F98D828D9984F9DCE23E4684780C436D2DD72B60F68854F0311CA67E8
102423F8D6C04A46F40814AD7D2C61C146E060B48BC56F701CE91B23F882D2F5AF4857B45560624
D758D3CA255AB83FEF1C2783CC37007D35AB5C9D158BDAE9F262536B93C509B8630A0809BDAE6
550027C00042F40BC881B53B29CAE10E0B4EF38DE9AD3C0161058EDA320F2D8832E3483FE9566
15CFE0F0D77F2BE9BDCCE45B80103936DF2E57D1B830096887B4E32C7AE8B9C52485A0D449C30C8
6D6D69BB5787537F6C6450814E12379B24454A25856D69AC5C4C60BF9DB9F022B79A39B59EF8965
5E23A4FPA42719C7CD22C798373E4EC07F083050B14974DEC0B753F69E3540D2FFC327BCD3E798
B49E9C0C87097C4DFE3F84ABC043C112C1B94D9828C1FBF3A339D7BC6E371DD7488B5B4DFD65C
43CD104DF95126C8F1E66283C574882DCE8BD6A5CF8E87259E66DECAB655E7CF24BF72B310B5428
421C74ADA64FDCCA31EFAF9682DFD3DF8E826DA969A94328FB49EF01DD593AF39696375D15A200A
3321E654D1508A491E8911A9E37B26498C34F706386F726E236C53027AB847FFC7C68E81214A
8DD01BF6190276C0DFBC9E0B5E34AAE9A674274DB239346C328C8DC2C198702211867AE3BEC62F7D
81E8505647887762E2FD6D40D98C746C570F16CBC3BAF1F37BBB58CE7DC1C46385D5B1AAE096A8AB
E47525C2CCB0DB0DE71A91F8B74A2B49453C22F2B2A5E0F3E48384C418097069EAE1BF79CF7F842
61CBE42E9AA759A5334E3E351001B01B0B68CA749973B344D3C25B03AD3C02CBEDD17F06094D8C
B80C0842BC938331B27E6C11A9E172A3A203EA55686CF4A10F810ED573CE98BF8375AEC53E413F1
0BE2984524982A1C1E459E552934660AE0B95C64AC5F73C088D95F7AE238850DD0BDEF921060E4B
C1E4D11F6683A9785387298413B45407F4F7ED54D899AAC7B31CC096FADD61B5A8810D0C29547B59
A77E115210947802A2E221F2F902E2BC8E6291884EF72200743877AAB5EA9A2C5934F9B1F089A
FEF13873D4B180DBA5F9CC4BACCEC468610C9485CFE7AC84817E65A2524052278BE780BC3F624A8
B4E0DEFF8E8219E9C839AFF50D1F4F08050555C23210B4F41D8118256C35251DD5DC44594D862F
59DC435A89AE2434164DE81FF8CA087C863BA1706E490E18D5FDICFE1D3A138EAD13E6886CEFC
98886B7AF828C9281B940FA760A2969541E63B945A863E1021A0812EA0060CD7F7834FED06CE20
627CC956D515C264035254B5FAF16880C102401FBB88BAF6740DFFED047B7C5D468097D33CA6
90474A9F1E1CC0563A5654C7BC7201232F8F16054D85F9FAD7F716E87167FC03D

PS C:\Shared\Tools\Rubeus>
```



Establishing Persistency

◆ **Persistency involves:**

- ◆ **Scheduled Tasks:** Setting up tasks to execute payloads periodically, ensuring continued access.
- ◆ **Service Registry Modifications:** Adding or modifying registry keys to execute malicious software at system startup.
- ◆ **GPO Modifications:** Adding or modifying Group Policy to execute malicious software on login at targeted machines.
- ◆ **Account Manipulation:** Creating or modifying accounts to ensure they can be used to regain access.
- ◆ **Golden Ticket:** With domain admin rights, attackers can create a ticket-granting ticket (TGT) that gives them authorization to any service in the domain.
- ◆ **Silver Ticket:** Similar to the Golden Ticket attack, but it targets service tickets (ST) for specific services rather than creating a TGT.





Privilege Escalation, Lateral Movement & Persistence

◆ Sample Basic Tooling

- ◆ Responder - LLMNR/NetBIOS/mDNS responder: <https://github.com/SpiderLabs/Responder>
- ◆ Impacket - python implementation of network protocols (SMB, Kerberos, LDAP): <https://github.com/fortra/impacket>
- ◆ BloodHound - map AD relationships/attack paths: <https://github.com/SpecterOps/BloodHound>
- ◆ Mimikatz - memory extraction, Kerberos ticket manipulation (DCSync/DCShadow techniques): <https://github.com/ParrotSec/mimikatz>



Reporting & Debrief

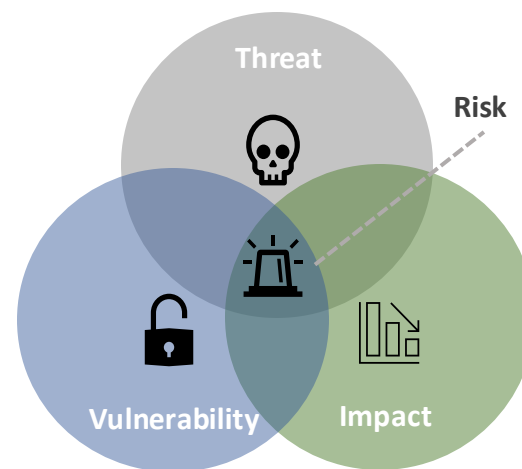


Closure phase | Reporting & Debrief

A story-drive report that contains the RT flow of progress, and its ability to execute or meet the predefined goals with the following additional sections:

- ◆ Executive Summary
- ◆ Attack path diagrams, specific attack-flow diagrams
- ◆ Map techniques to MITRE ATT&CK for defender alignment
- ◆ A separate section with findings discovered towards meeting the predefined goals.

Rating and Score	Impact	Likelihood
CRITICAL (5)	Extreme	Almost certain. Knowledge of the vulnerability and how to exploit it are in the public domain.
HIGH (4)	Major impact to entire organization / regulatory violation.	Relatively easy to detect and exploit by an attacker with little skill.
MEDIUM (3)	Noticeable impact to line of business if exploited.	A knowledgeable insider or expert attacker could exploit the vulnerability without much difficulty.
LOW (2)	Minor damage if exploited	Requires considerable expertise and resources.
INFO (1)	Does not represent an immediate risk on its own	Not likely to be exploited on its own





Reporting & Debrief

- ◆ Include prioritized remediation: quick wins, medium fixes, long-term projects.
- ◆ Run a debrief workshop with blue team and executives.
- ◆ Deliver a clear timeline: actions, timestamps, detected vs undetected events.
- ◆ Share reproducible detection recipes (SIEM queries, EDR rules).





Ethical & Legal Consideration



Ethical & Legal Consideration

- ◆ Always **work under explicit written authorization and scope**.
- ◆ **Adhere to privacy laws and data handling requirements**.
- ◆ **Avoid destructive or disruptive techniques** in production.
- ◆ **Maintain clear evidence chains** for post-engagement analysis.
- ◆ **Communicate transparently** with leadership and legal teams.



Thank you!

