Re-defining Success of Ground Cyber Assessments

Brandon Bailey
Cyber Security Subdivision (CSS)
Cyber Assessments and Research Department (CARD)

GSAW 2020
Cyber Working Group

brandon.bailey@aero.org
240.521.4326 (c)

© 2019 The Aerospace Corporation

Traditional Government Evaluation Standard

- The U.S. federal governance structure for general Information Technology (IT) based cybersecurity has made strides in recent years with the maturation of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and/or Cybersecurity Framework (CSF)
  - *The NIST cybersecurity maturity standards and guidelines help organizations to improve their cybersecurity measures and best practices but these are not directly applicable to the space domain, especially the spacecraft*
    - NIST guidance has some applicability on the ground segment
      - *Space Overlay does exist (Appendix F CNSSI 1253)*
      - *MDA Software Assurance Overlay Released June 2019*
  - *NIST is currently authoring a white paper on cyber considerations and applying CSF for space systems (likely to focus on satellite technology)*
- While efforts have been made, and are currently ongoing, to mold these frameworks for space systems, uniformity is lacking and updated standards and guidelines for space are likely warranted
  - *Maybe a ground system specific overlay?*
- Many assessments are compliance based against laws, NIST RMF and/or CSF
  - *ATO is the definition of success but ATO being granted does not mean security*
    - Personally have successfully exploited ground systems operations that could lead to severe mission degradation and **EVERY** system had an ATO!

Attackers do not care if you are compliant!!

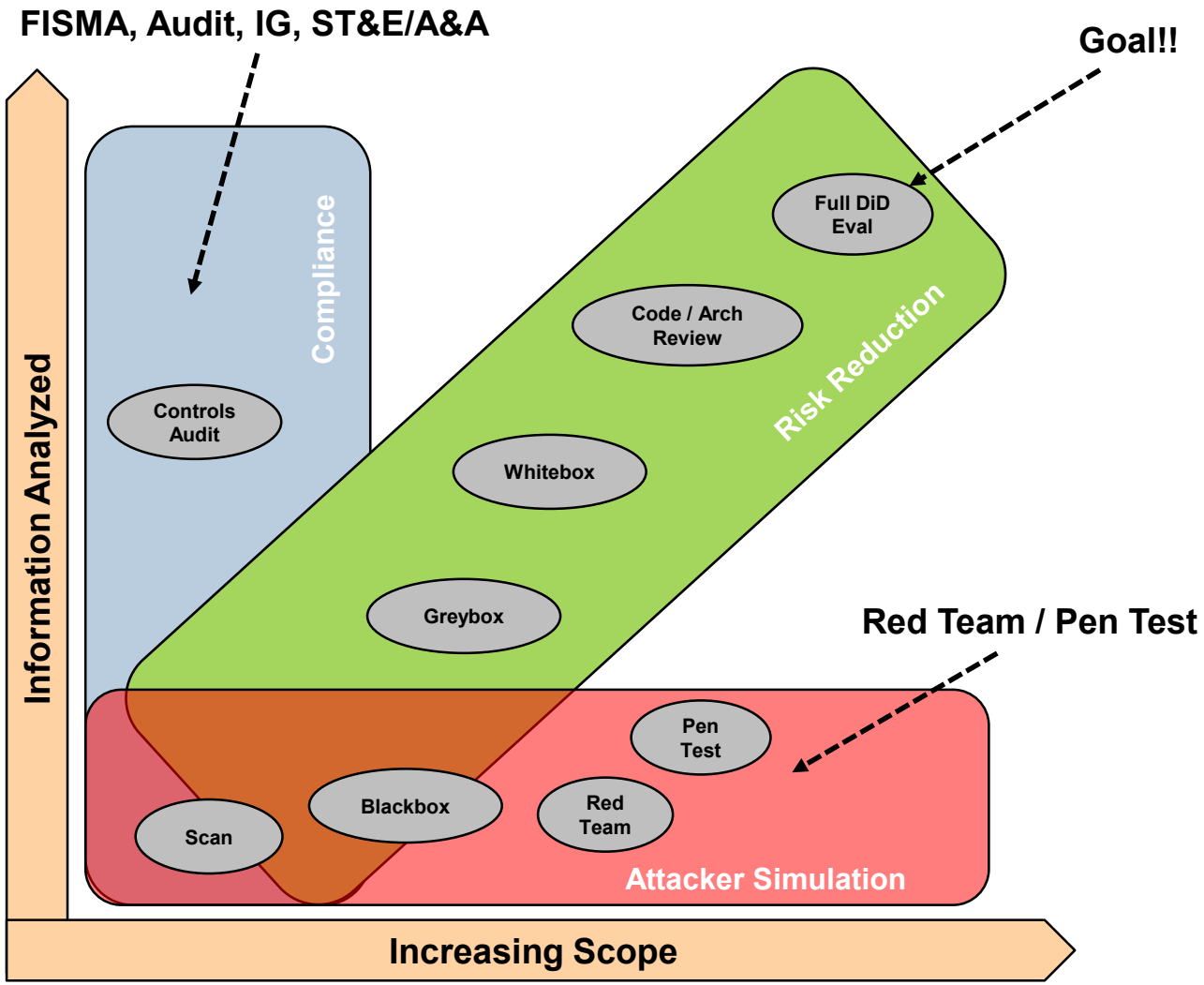
NO INHERENT RELATIONSHIP

	Compliance	Security
Provable	✓	✗
	WHERE MOST PROGRAMS LIVE	
Disprovable	✓	✓

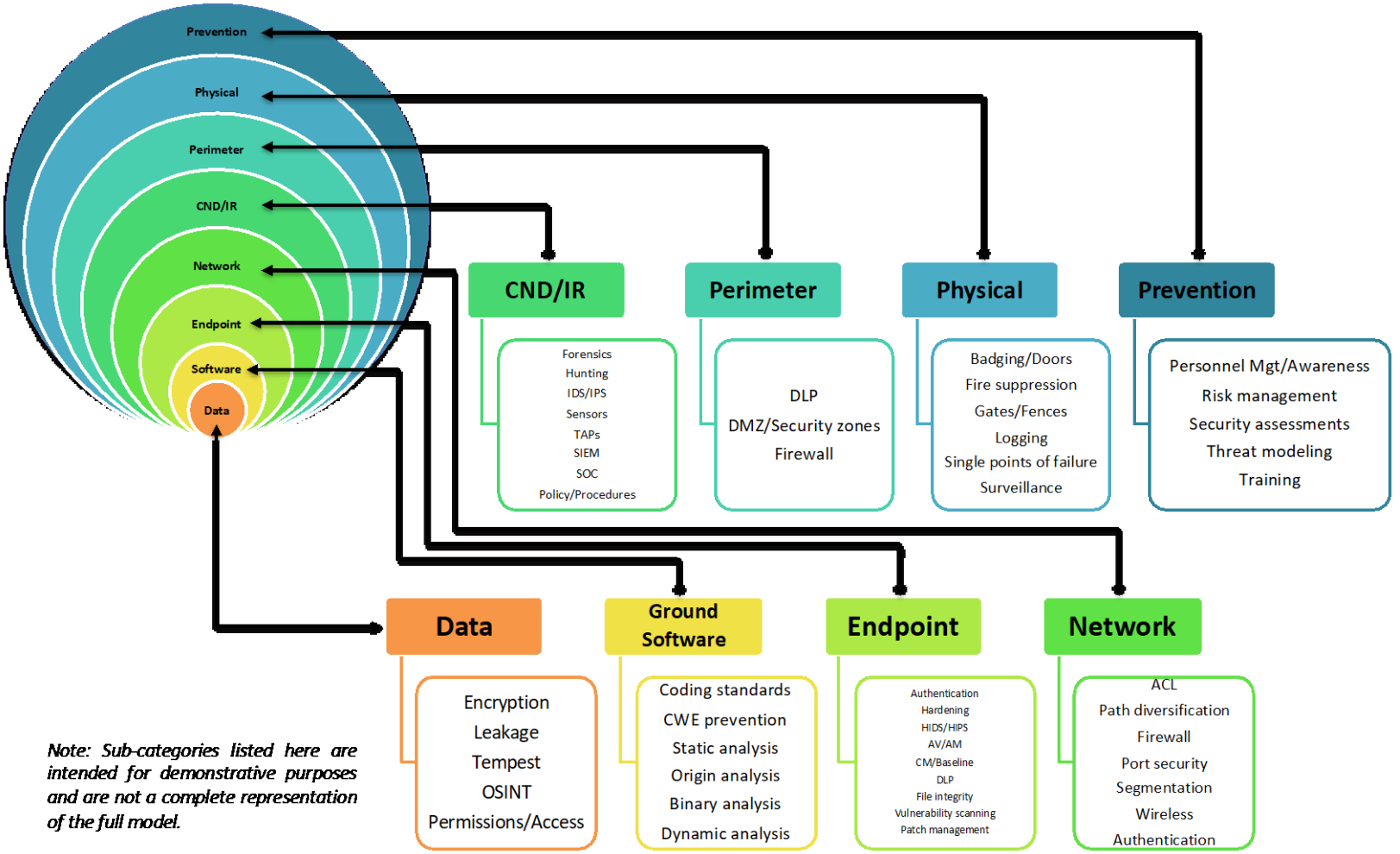
Comparison of Assessment Types

Recommended Approach for Assessment	Focus of Other Assessment Type Activities
Fully evaluates all layers of architecture and the mission critical assets and determine operational security risk posture	**FISMA:** State of Regulatory Compliance (per NIST 800-53). Usually high level.
Identify vulnerabilities, their exposures both internal and external, and impacts those vulnerabilities will have on the mission	**Audits:** Detecting Fraud or error/evaluate adequacy of controls
Comprehensively assess all factors (backups, COOP, ICS/SCADA, Infrastructure, etc.)	**IG**: Examine actions of Government Agency; Focus on misuse
Provide deliverables/products that will guide the customer on the most appropriate and beneficial mitigations	**ST&E/A&A:** Evaluates compliance for Assessment & Authorization. System specific with ATO being signed.
Assist Mission elements to understand/mitigate security risks based on exposure and threat	**Red Team**: Simulate attack on asset to discover vulnerabilities. Unannounced and narrowly focused.

Comparison of Assessment Types (cont.)



Example: Ground Segment DiD



Note: Sub-categories listed here are intended for demonstrative purposes and are not a complete representation of the full model.

Goal is to evaluate <u>implemented</u> controls at <u>all layers</u>.

Mission Focused Ground Truth Technical Evaluation!!

Generic Assessment Objectives

- Not compliance focused, but risk-focused using technical ground truth
  - *Cyber assessments and mission assurance go hand in hand*
- Assess the survivability of the mission, organization, architecture, systems, and assets from a cyber perspective using available threat information
- Identify cyber-related mission vulnerabilities within an organization, architecture, system or assets that may adversely impact the mission's ability to execute its assigned missions
- Evaluate the defense mechanisms in place throughout the architecture and determine if they are adequate based on the network and systems architecture deployments
  - *Defense-in-Depth is key!*
- Increase the customer's awareness of potential vulnerabilities and the impacts if exploited (*i.e. Not that you fail NIST control AC-4*)
- Provide actionable recommendations to mitigate or eliminate identified vulnerabilities

Success is providing decision makers with actionable ways to reduce cyber risk on ground infrastructure by understanding architecture, limitations, and budget.

Approach and Methodology

- Cyber security applies across all phases of operations and throughout all layers of the architecture
- Must understand the mission and threats to the mission
- Active and/or passive testing techniques could include a combination of three principal methods:
  - *Analytic/Tabletop Analysis (e.g. Threat Modeling)*
  - *In the Lab Testing (modeling-simulation environment)*
  - *On-Site and/or On-Network*
- Determine critical assets, model the "mission thread" that these critical assets use to enable the mission – then do a selective "deep dive" on potential points of vulnerability to cover:
  - *Supporting Infrastructure: (Layer-2/Layer-3 Network Devices, Controlled Interfaces/Firewalls, Cybersecurity Defense (CND) mechanisms, Threat Hunting, etc.)*
  - *Industrial Control Systems/SCADA*
  - *Software Security Evaluation*
    - Analyze the software code base which supports critical assets and mission threads
  - *Processes and Procedures*
  - *Survivability (includes measures to enhance security, redundancy, and physical diversity)*

Passive Cyber Assessments

- Traditional non-compliance based cyber assessment methods (scanning, penetration testing, red/blue team activities) have evolved alongside traditional networks
  - Strategies designed for typical enterprise networks with modern infrastructure
    - Networks with ample bandwidth
    - Operating systems with a baseline security configuration & tools
  - These assessments rely on interaction with the environment to probe, scan, and potentially exploit target systems
    - Active assessments carry inherent risk to the target system, especially for legacy
  - Essential tool for the toolkit, but not all environments are built the same
- Ground system owners sometimes have highly specialized network environments that support a range of legacy systems
  - Minimal bandwidth, end-of-life operating systems
  - Fragile infrastructure housing critical mission systems
  - Networks that cannot be easily improved due to budget constraints, mission phase, or other organizational drivers

Passive Cyber Assessments (Aero's Approach)

- Aerospace continues to develop several capabilities to define risk for fragile/mission critical systems
  - *Rely on collecting information to perform offline analysis for various purposes*
    - DCO 2.0: Flexible toolkit for cyber defense using ML/AI
    - Commercial tool purchased to create powerful network models
    - Immortal Snail: Aerospace prototype for tracking cyber vulnerabilities offline
    - SW Security: Running SCA, Binary, Origin, Dynamic
  - *Correlate many desperate tests into overall technical risk assessment*
- **DCO 2.0** can integrate with SIEM and be fed with network traffic captured from a spanned or tapped interface(s) to identify anomalous traffic patterns
  - *Using machine learning, to assess GBs/TBs of network traffic at near real-time*
  - *Can decode space protocols for space-based ground IDS*
- Commercial tool can build an offline model of the target network to identify network traffic paths that could be exploited
- **Immortal Snail** imports vulnerability scans or allows for customized hosts to track emerging vulnerabilities
  - *In the future it will support engineers by alerting to increased risks without requiring new vulnerability scans*

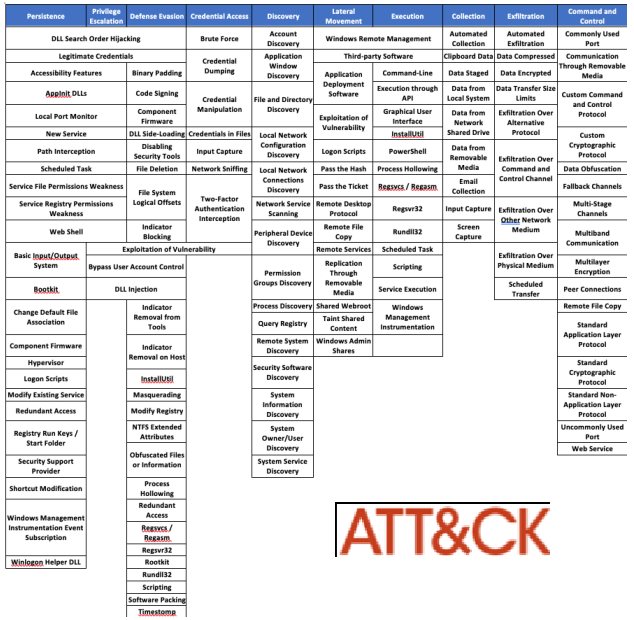
Active / On-Network Assessment

- To augment the passive assessments, more active approaches should be used to emulate attackers' TTPs
  - *Using threat intelligence, unclassified and classified TTPs can be used to drive on-network activities*
    - Minimum the ATT&CK framework (https://attack.mitre.org/) can be leveraged
    - TTPs are how the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration or destruction and at every step in between.
- Most thorough cyber assessment approach is a combination of passive, active/red teaming, and software assessments to evaluate DiD (a.k.a. purple teaming)
  - *Provides representative threat emulation of both outsider and insider*
  - *Many vulnerabilities are only identifiable on live systems with real data flowing*
  - *Remember attackers use TTPs and not attack a single NIST control or lack thereof*
- Can be augmented for fragile space systems
  - *If full blown active on-network testing is not permitted, you can leverage virtualization to replicate as many critical servers in a lab (e.g. physical to virtual, virtual machine exports, docker containers, etc.)*
- Goal is to provide evidence to support impact criticality statements
  - *Want to consider all controls in place and understand vectors to exploit vulnerabilities*

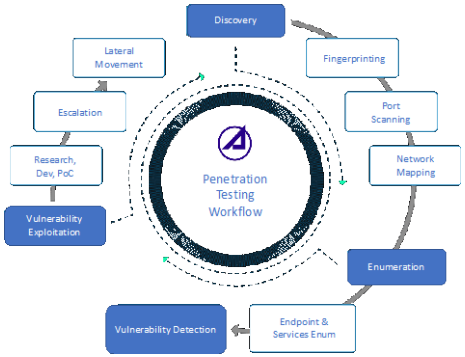
Network Based Attack Approach (Aero's Approach)

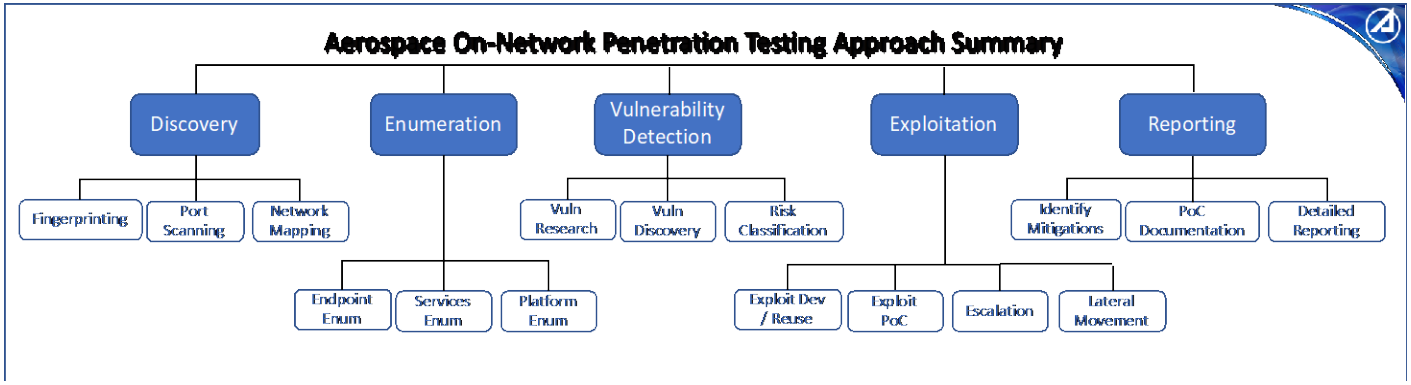
Demonstrate Exploitation Scenarios

- Threat-based pen testing provides a way to perform adversary emulation
  - *Emulate the techniques of an adversary that's most likely to target the environment we are testing (ATT&CK can help)*
  - *Focus on the behaviors of those techniques instead of specific implementations*



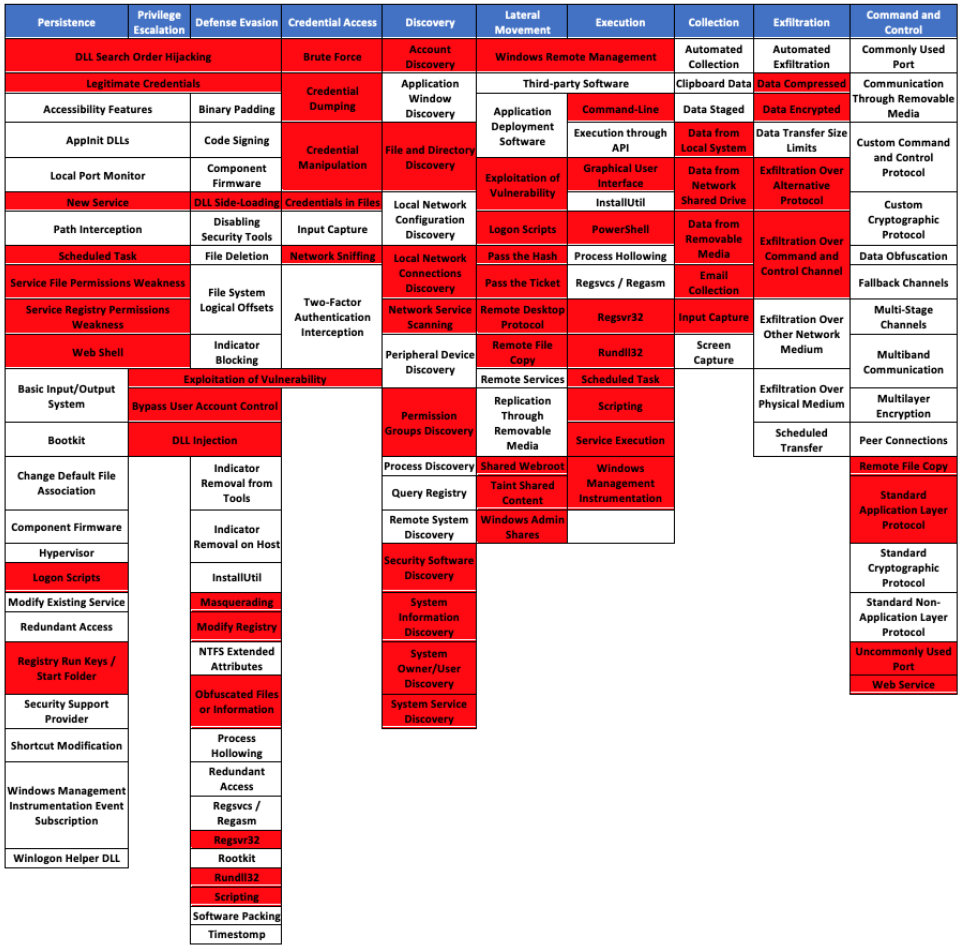
- It's beneficial to understand all attack/threat vectors and attempt to emulate real TTPs to circumvent security controls
- Typical approach is discovery, enumeration, vulnerability detection, exploitation, escalate, lateral movement to crown jewels then exfiltrate / simulate D5 (deceive, degrade, deny, disrupt, destroy)





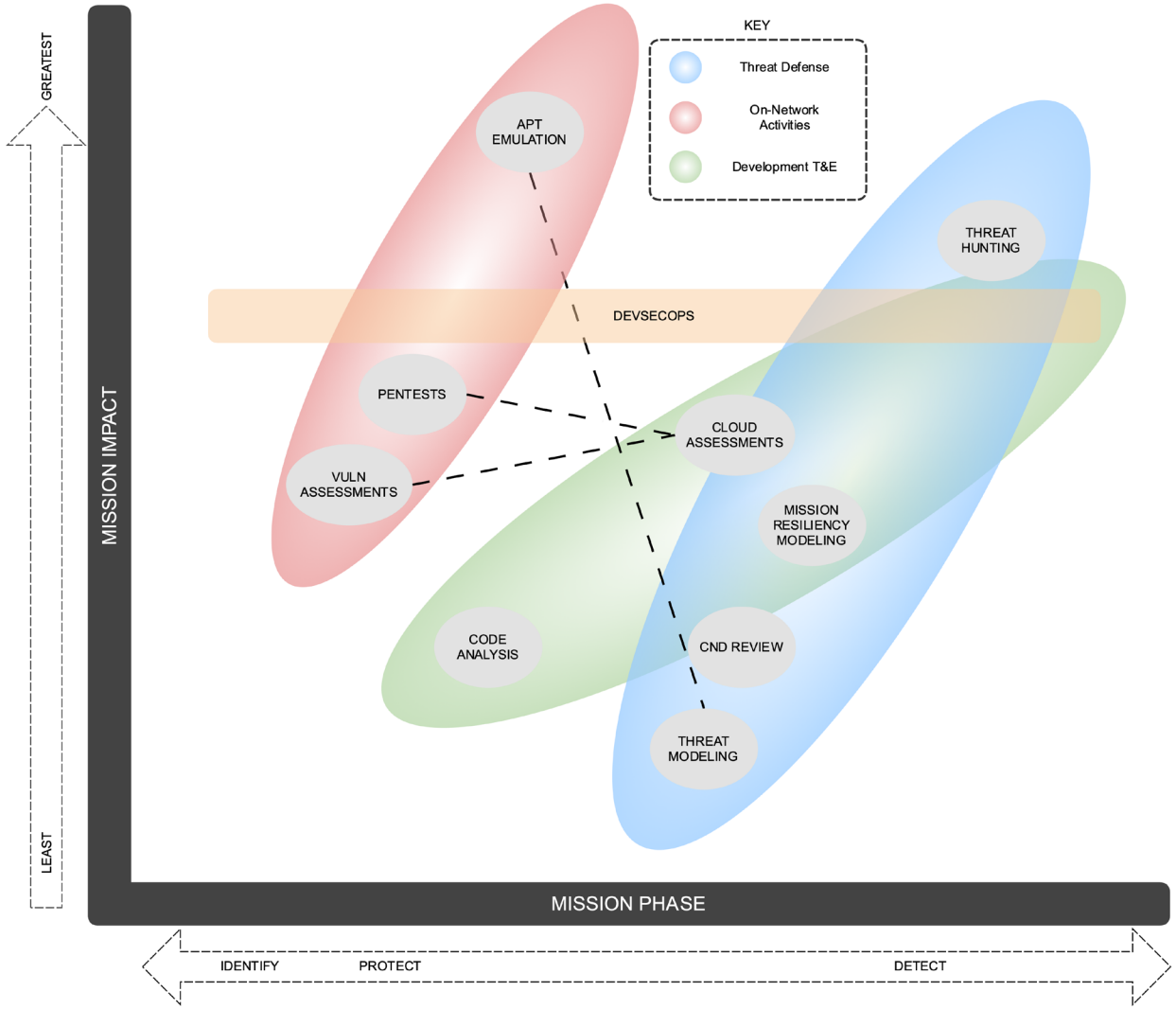
Example Ground System TTPs

- Emulating TTPs requires an arsenal of knowledge and tools
- No two missions are identical
  - Tools and methodologies that work on one system may not yield satisfactory results on another
- Every environment is different and must be approached in a methodical manner
  - Attention to detail is crucial
  - Being able to identify tiny differences between configurations can mean the difference between a successful exploit or not
- Think outside the box and don't hesitate to attack in ways never been done before
  - Just as a real attacker would in the real world. **But you must be careful when operating in a highly fragile environment!**



Cyber Assessments & Threat Hunting

Aero's Assessment Methods within CARD



Cyber Assessments Range in Scope and Goals

Cyber Assessments & Threat Hunting (cont.)

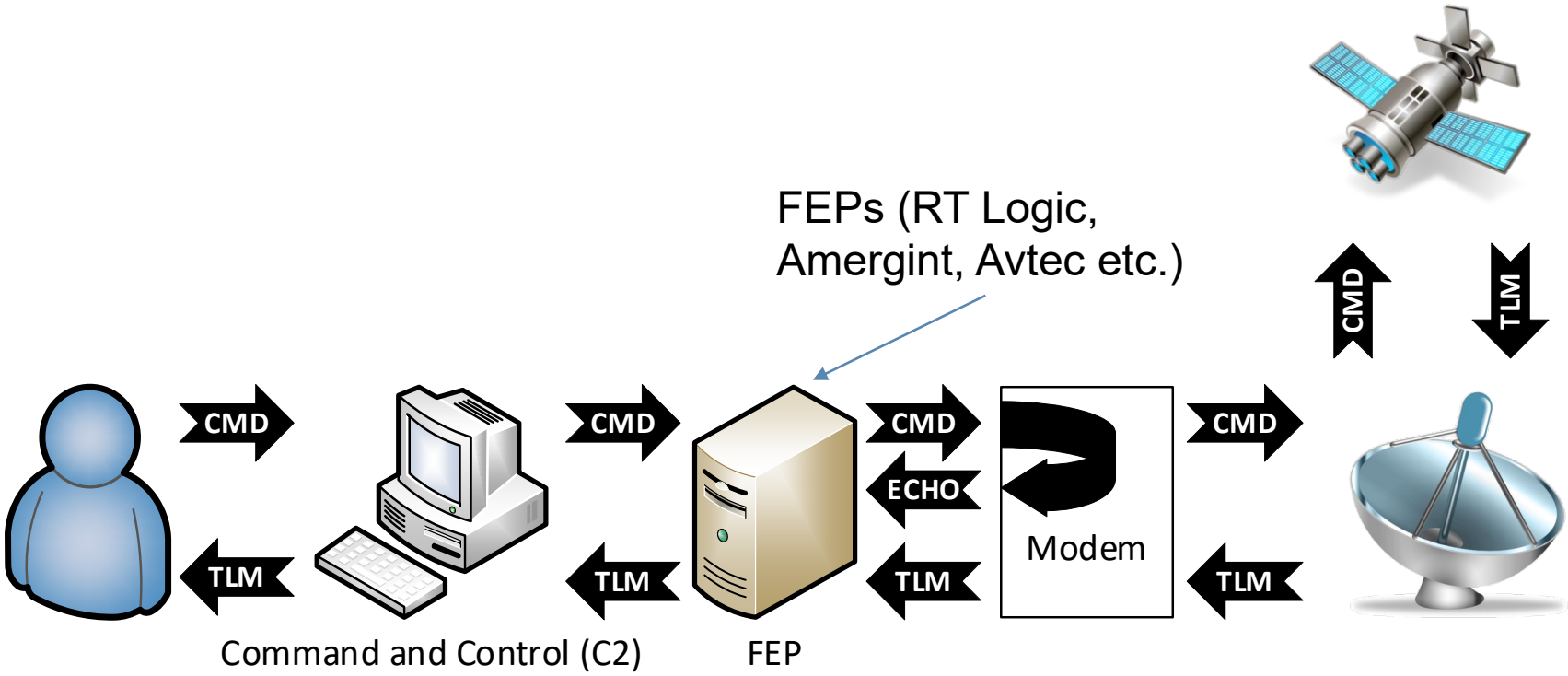
Method Decomposition

Development T&E		On-Network Assessments			Threat Defense			
Code Analysis	**DevSecOps**	**Vulnerability Assessments**	**Penetration Tests**	**APT Emulation**	**Threat Modeling**	**CND Review**	**Mission Resiliency Modeling**	**Threat Hunting**
Passive	**Active**	**Passive/Active**	**Active**	**Active**	**Passive**	**Passive**	**Passive**	**Active/Passive**
Static Code Analysis	CI/CD Pipeline Security	Network Recon	Targeted Exploitation	Threat Modeling	Threat Intelligence	Architecture Review	L2/L3 Config Review	Capability Hunt
Code Fuzzing	Automated Testing	Vulnerability Scanning	Privilege Escalation	Threat Intelligence	Critical Mission Functions	Tool Studies	Threat Path Analysis	Adversary Hunt
CWE Prioritization	Continuous Monitoring	Vulnerability Remediation	Common Attack Paths	Mission Threat Scenarios	Interface Analysis	Gap Analysis	Enclave Visibility	Target Hunt
Code Source Analysis	Post-Mortem Analysis	Passive Vulnerability Collection	Password Cracking	ATT&CK/Kill-Chain Mapping	Defensive Layers	Data Handling	Defensive Layer Hardening	Infrastructure Hunt
Reverse Engineering	Continuous Compliance	Assessment & Authorization	Physical-to-Virtual Testing	Custom Exploitation	Staff Interviews	Hardened Config	Mission Critical Remediation	ATT&CK/Kill-Chain Mapping

Real Life Example

Front End Processors

Scope for this Example



FEP: Commanding & Telemetry

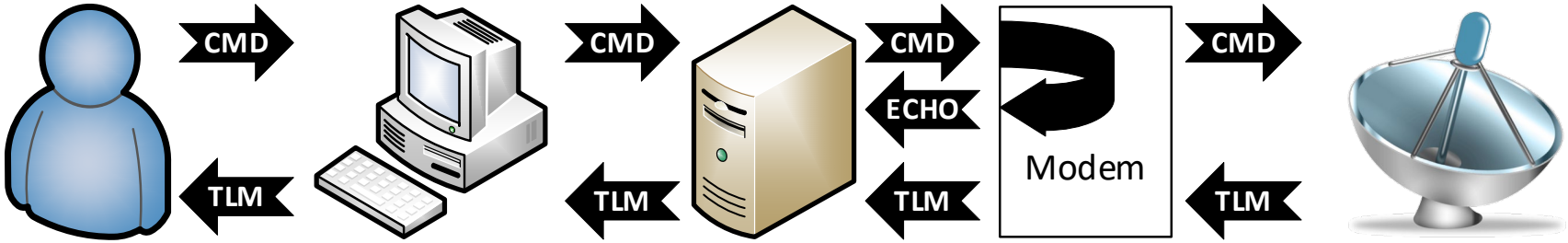
- Commanding
  - *Command and Control (C2) Systems automate user processes:*
    - Send command sequences
    - Translate mnemonics to binary commands
    - Set limits on commanding
    - Store logs of commands sent and telemetry received
  - *C2 controls the FEP*
  - *Modem converts digital signal to analog signal (modulation)*
  - *Transmitter amplifies and transmits RF signal*
- Telemetry
  - *Receiver collects and amplifies RF signal.*
  - *Modem converts analog signal to digital signal (demodulation)*
  - *Command and Control (C2) Systems automate user processes:*
    - Translate frames/sub frames of telemetry into calibrated data (decomm)
    - Set limits on telemetry
    - Store logs of commands sent and telemetry received

Sample Attack #1 during PenTest

The software performs actions in the server's operating system using calls build in the "Python" scripting language. Several scripts exist in the URLs that execute tasks in the OS and return the output to the application.

The calls performed by these scripts are passed to the OS without the use of **input validation** or **any authentication** at the application/OS level. The use of these scripts creates a semi-shell environment where a user can execute many OS commands through the web browser.

Input Validation & Lack of Authentication Vulnerabilities

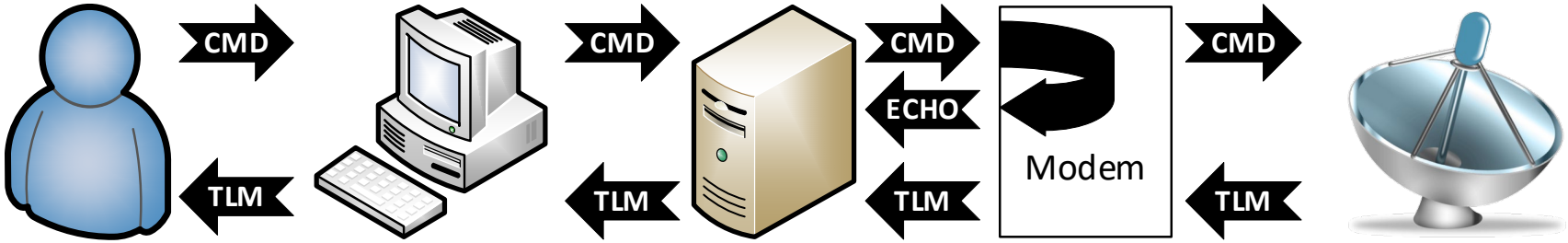


Sample Attack #2 during PenTest

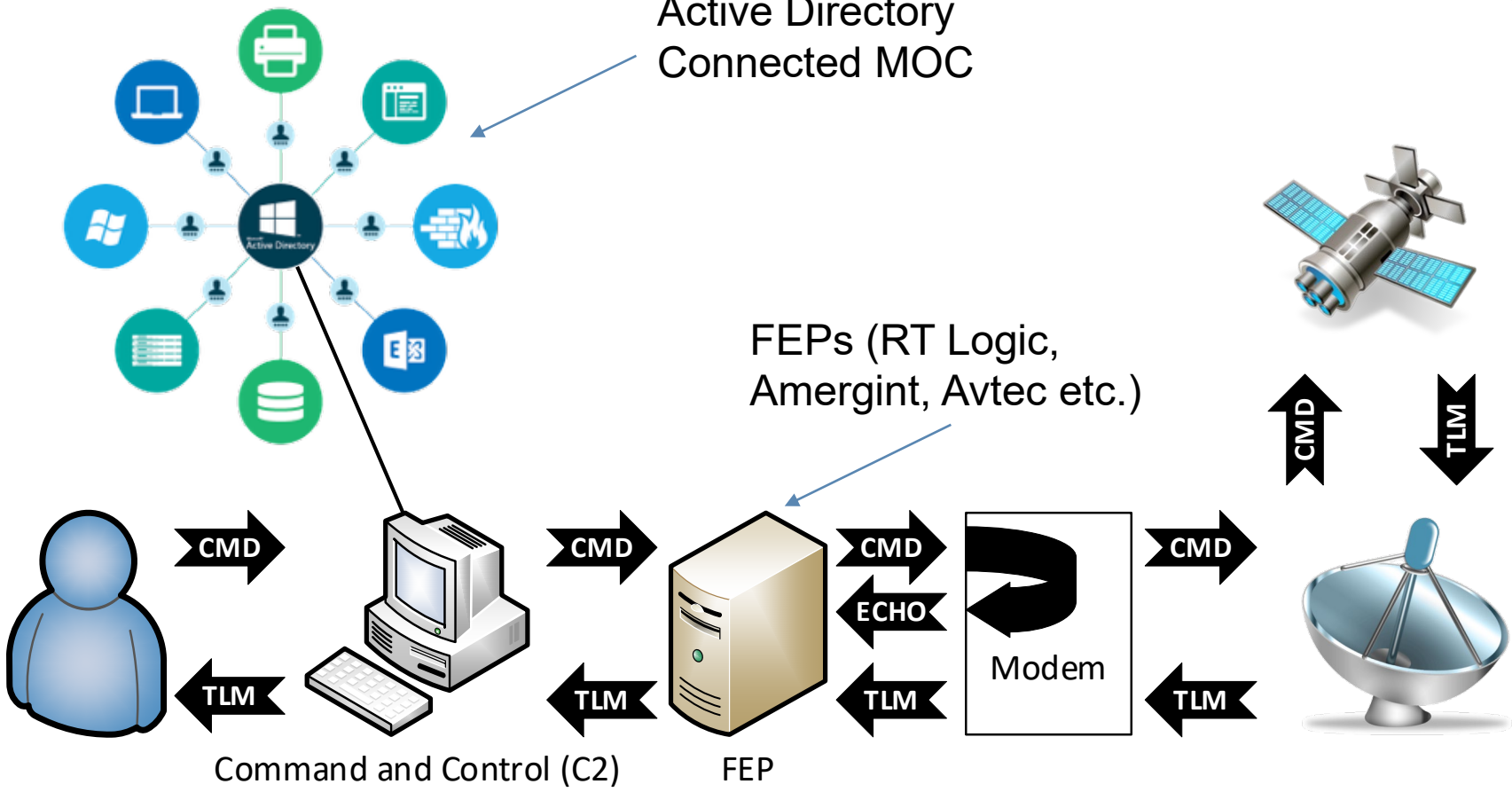
FEP intended design…. "*Just write the message to the socket, and read the reply. In fact, if you are so inclined, you can telnet to port xxxxx and enter the messages directly.*" – Vendor Docs

Therefore, anyone with access to the network has the capability to send commands to these ports and reconfigure the FEP **unauthenticated**. If used as an attack vector, it affects the availability and integrity of the FEP system.

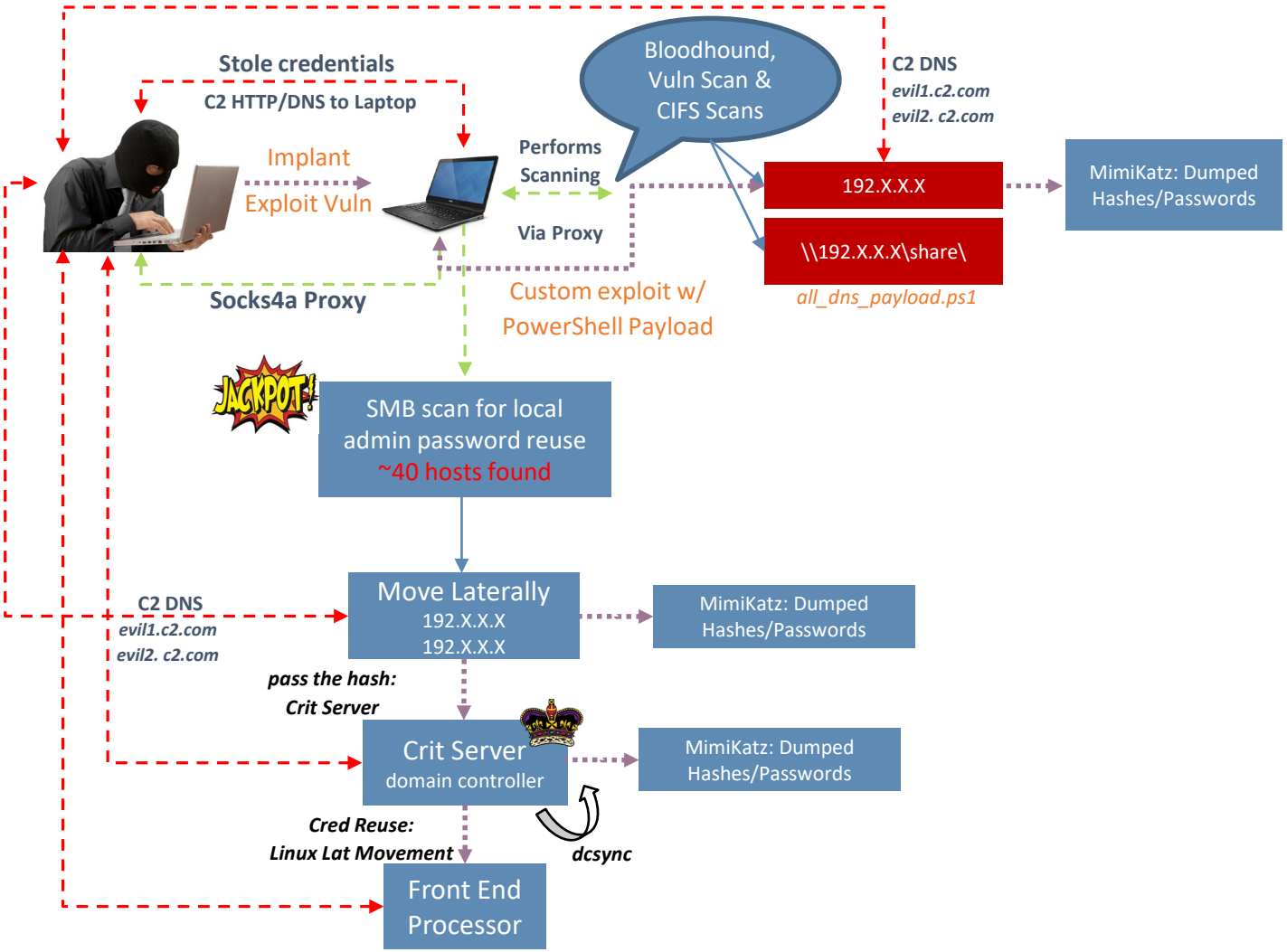
Unsecure Design = Lack of Authentication
Vulnerabilities



Scope for this Example

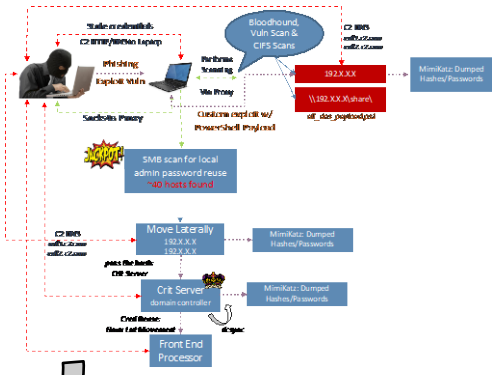


Full TTP Emulation



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	Multilayer Encryption
	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting			
Bootkit	DLL Injection					Service Execution		Scheduled Transfer	Peer Connections
Change Default File Association		Indicator Removal from Tools		Process Discovery	Shared Webroot	Windows Management Instrumentation			Remote File Copy
Component Firmware		Indicator Removal on Host		Query Registry	Taint Shared Content				Standard Application Layer Protocol
Hypervisor				Remote System Discovery	Windows Admin Shares				
Logon Scripts		InstallUtil		Security Software Discovery					Standard Cryptographic Protocol
Modify Existing Service		Masquerading		System Information Discovery					Standard Non-Application Layer Protocol
Redundant Access		Modify Registry		System Owner/User Discovery					Uncommonly Used Port
Registry Run Keys / Start Folder		NTFS Extended Attributes		System Service Discovery					Web Service
Security Support Provider		Obfuscated Files or Information							
Shortcut Modification		Process Hollowing							
Windows Management Instrumentation Event Subscription		Redundant Access							
		Regsvcs / Regasm							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

ATT&CK framework overlapped with previous exploitation scenario

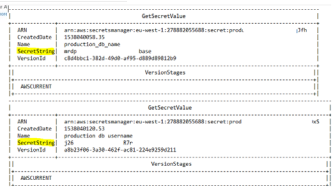


What About Cloud & DevSecOps?

Executed AWS Key Theft and Utilized to Extract Mission Data

- ✓ Attacker compromises developer laptop or Insider performs GitLab CI Pipeline Code Injection

DevOps should include constant pen testing and adversarial assessments using automated mechanisms to evaluate the application as it evolves



aws cli

Enumerate EC2, S3, Lambda, Security Groups, Subnets, Secrets

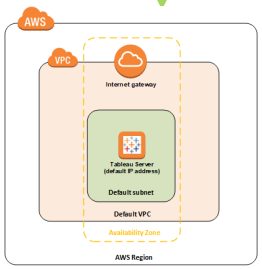
Create EC2 Instance

```
aws ec2 run-instances --image-id ami-
047bb4163c506cd98 --iam-instance-profile
Name="oprah-ec2-instance-profile-
production" --key-name audit.prod --
subnet-id subnet-0342b23d200c7afea --
security-group-ids sg-066fbd7a33d14c4e4
--associate-public-ip-address
```

Port 5432
Postgres


```
aws ec2 authorize-security-group-ingress --group-id
sg-066fbd7a33d14c4e4--protocol tcp --port 22--cidr
0.0.0.0/0

aws ec2 authorize-security-group-egress --group-id
sg-066fbd7a33d14c4e4--protocol tcp --port 22--cidr
0.0.0.0/0
```



Attack scenario for DBs in VPC

- ✓ Compromise Keys (previous slide GitLab CI)
- ✓ Backdoor automation-user account for GUI access (not required)
- ✓ Recon and dump secrets
- ✓ Create EC2
- ✓ Modify SG for SSH
- ✓ Access DB using “Secrets”

Summary

Continuous Monitoring Strategy - Moving Forward

- Using these aforementioned types of cyber assessments will improve security in the following ways:
  - *Discovers weaknesses in systems that may arise from misconfigurations or poor design*
  - *Discovers vulnerabilities that have not been patched*
  - *Discovers changes from configuration controlled baseline (what's ground truth?)*
  - *Ability to classify risk using network exposure of vulnerability and mission impact*
- There should be wider adoption of in-depth technical assessments in operational environments
  - *Takes skilled and knowledgeable assessors and **willing participants***
- Goal should be threat driven risk identification and provide actionable guidance to system owners to improve system security and reduce risk
  - *Remember attackers use TTPs and not attack singular NIST control, DiD critical!!*
- Assessment of ground systems can pose unique challenges and may require unique passive techniques
- Aerospace is continuing to develop unique capabilities to effectively conduct passive cyber assessment
  - *Best value is combining passive with on-network techniques to discover vulnerabilities many scanners or paper assessments will miss and help articulate true risk to the mission*