



Forensics 2: Incident Response

Kresten Jacobsen

Intro to System Security

Goals

Prevention

Detection

Recovery

C-I-A

Confidentiality

Integrity

Availability

Threats

Snooping

Modification

Spoofing

Repudiation of Origin

Denial of Receipt

Delay

Security Policies

Requirements

- Common understanding (implicit / explicit)
- Trust (in people and computers)
- Assumption (that policies are enforced)

Policy types

- Confidentiality
- Integrity Policy
- Availability Policy

Incident Response - terms

- Attack
 - *a sequence of actions that create a violation of a security policy*
- Goal
 - *what an attacker hopes to achieve*
- Target
 - *the entity that the attacker wishes to affect*
- Multistage attack
 - *an attack that requires several steps to achieve its goal*
- Attack surface
 - *the set of entry points and data that the attackers can use to compromise a system*





Incident Response - phases

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Follow-up / Lessons Learned

Incident Response - Preparation

- Verification of the system in place
- Examine procedural and operational controls
- Is the system in fact installed and operated as expected
- Example, is the firewall even enabled?
- Penetration testing methodologies / frameworks (OWASP, ATT&CK)

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK™

ATT&CK - Matrix

Comprehensive matrix, containing *tactics* at the top, and *techniques* listed under each tactic.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Applnit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing	Execution through Module	BITS Jobs	DLL Hijacking	Corrupts After Delivery	Forced	Network Sniffing	Remote Desktop	Data from Removable	Domain	Exfiltration Over Physical	Inhibit System

