Vulnerability Management

Breach and Attack Simulation

Klaus Möller

WP8-T1

Webinar, 15th of September 2021

www.geant.org
The Road Ahead: Breach and Attack Simulation

• What is Breach and Attack Simulation?
• Modelling Attacks
• Adversary Emulation
• Live Demonstration
• Wrapping Up
Motivation

- Also/better called: “Adversary Emulation”
- Marketing: Breach and Attack Simulation (BAS) goes beyond vulnerability assessments, penetration testing, and red teaming by offering automated and advanced breach simulation
- "... proactively predict attacks, validates security controls and improves SOC analyst response"
- Lots of phrases that don’t help if you don’t know about it already
- What does it do then? And how?
  - How does it compare to Penetration Tests and Vulnerability Assessments?
  - Or high-level (table-top) exercises (like CLAWS)?
First

- To emulate an attacker, we have to know how an attacker behaves
  - I. e. we have to observe real adversaries and their attacks on real networks
- Then, we need abstract the observations to a formal model
- Then, we can use this model to emulate adversaries on our network
Modelling Attacks
(Intrusion|Cyber) Kill Chain

7. Actions or Objections: The attacker meets his/her goal (e.g. stealing information, gaining elevated privileges or damaging the host completely)

6. Command & Control: Setting up controls so the attacker can have future access to the host’s network

5. Installation: Installing the actual malware

4. Exploitation: Once the host is compromised, the attacker can take advantage and conduct further attacks

1. Reconnaissance: Collecting information and learning about the internal structure of the host organization

2. Weaponization: How the attacker packages the threat for delivery

3. Delivery: The actual delivery of the threat (via email, web, USB, etc.)
Pyramid of Pain

- Threat Intelligence Concept
- Values low in the pyramid are easy to observe/counter
- But also easy to change for the adversary
- The higher up in the pyramid, the harder it is for adversaries to change
- Conversely, the effort needed to observe/deduce goes up also
Mitre ATT&CK

- An effort to document common tactics, techniques and procedures (TTPs) used in APTs
  - *Adversarial Tactics and Techniques based on Common Knowledge*
- A knowledge base of adversary behaviour based on observations of real incidents
- Broken down into
  - Tactics: What an attacker tries to accomplish at a given phase (goals)
    - See Kill Chain for comparison
  - Techniques: Behaviour that is used to accomplish the attackers target
- Also: A common taxonomy (compare CVE, et. al.)
ATT&CK and the Kill Chain

• Data in the knowledge base is organized in a matrix
• Tactics: Column (header)
• Corresponds roughly to a phase of the kill chain
• The objective the attacker tries to reach (the “why”)
• Rows of a column: List of typical techniques used (the “how”)
• There are different matrices covering different environments
  – Enterprise systems, Mobile, Industrial Control Systems
• Techniques are covered in detail on separate web pages
  – Including mitigations - against a technique
Sample ATT&CK Technique

T1136: Create Account

Adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialized access that do not require persistent remote access tools to be deployed on the system.

Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

Mitigations

<table>
<thead>
<tr>
<th>ID</th>
<th>Mitigation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1032</td>
<td>Multi-factor Authentication</td>
<td>Use multi-factor authentication for user and privileged accounts.</td>
</tr>
<tr>
<td>M1030</td>
<td>Network Segmentation</td>
<td>Configure access controls and firewalls to limit access to domain controllers and systems used to create and manage accounts.</td>
</tr>
<tr>
<td>M1028</td>
<td>Operating System Configuration</td>
<td>Protect domain controllers by ensuring proper security configuration for critical servers.</td>
</tr>
<tr>
<td>M1026</td>
<td>Privileged Account Management</td>
<td>Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems.</td>
</tr>
</tbody>
</table>

Detection

Monitor for processes and command-line parameters associated with account creation, such as `net user` or `useradd`. Collect data on account creation within a network. Event ID 4720 is generated when a user account is created on a Windows system and domain controller. Perform regular audits of domain and local system accounts to detect suspicious accounts that may have been created by an adversary.

Collect usage logs from cloud administrator accounts to identify unusual activity in the creation of new accounts and assignment of roles to those accounts. Monitor for accounts assigned to admin roles that go over a certain threshold of known admins.

Source: https://attack.mitre.org/wiki/Technique/T1136
Sample Attack Technique in a Simulation Tool

```python
attack_technique: T1136.001
display_name: 'Create Account: Local Account'
atomic_tests:
  - name: Create a user account on a Linux system
auto_generated_guid: 4db8abdb-e394-45f6-8785-b96fa1d811d2
description: |
  Create a user via useradd
  supported_platforms:
  - linux
input_arguments:
  username:
    description: Username of the user to create
type: String
default: evil_user
executor:
  command: |
    useradd -M -N -r -s /bin/bash -c evil_account #{username}
cleanup_command: |
  userdel #{username}
name: bash
elevation_required: true
```

Source: https://github.com/redcanaryco/atomic-red-team/tree/master/atomics/T1136.001
Mitre ATT&CK Threat Actors

- Database stores also Information about Threat Actor Groups
  - Like APT29, etc. - some (but not all) well known APT groups
  - Open source information - don’t expect something new here
- Using this information allows to mimic the behaviour of this groups in adversary emulation
  - ATT&CK is used by many, but not all, adversary emulation tools
- Caveat: Threat Actors change and adapt, information may thus may not always be accurate
  - Outdated
  - Not commonly known (yet)
Mitre ATT&CK Threat Actors

APT29

APT29 is a threat group that has been attributed to Russia’s Foreign Intelligence Service (SVR) since 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR, public statements included citations to Dark Halo, Mitre, and related actors. The techniques used by APT29 are referred to the tactics involved in this campaign as UNC2452, Mitre, and NOBELIUM.

Associated Group Descriptions

- Dark Halo
- NOBELIUM
- UNICIST

Techniques Used

- Domain ID: T1548
  - Name: Abuse Elevation Control Mechanism: Bypass User Account Control
  - Use: APT29 has bypassed UAC.

- Domain ID: T1687
  - Name: Account Discovery
  - Use: APT29 obtained a list of users and their credentials.

- Domain ID: T1098
  - Name: Account Manipulation: Additional Cloud Credentials
  - Use: APT29 has added credentials to OAuth.

- Domain ID: T1098
  - Name: Account Manipulation: Exchange-Email Delegate Permissions
  - Use: APT29 added their own devices as alias administrators, allowing it to obtain copilot additional permissions (such as Mail and Application or Service Principals).

- Domain ID: T1583
  - Name: Acquire Infrastructure: Domains
  - Use: APT29 has acquired C2 domains.

- Domain ID: T1560
  - Name: Archive Collected Data: Archive via Utility
  - Use: APT29 used 7-Zip to compress stolen data to extirpation.

Software

- ID: 56502
  - Name: AdFind

- ID: 56504
  - Name: CloudDuke

- ID: 56714
  - Name: Cobalt Strike
  - Reference: Account Discovery: Domain Account, Domain Trust Discovery, Permission Groups Discovery: Domain Groups, Remote System Discovery, System Network Configuration Discovery

- ID: 56714
  - Name: CloudDuke

- ID: 56714
  - Name: Cobalt Strike
  - Reference: Account Discovery: Domain Account, Domain Trust Discovery, Permission Groups Discovery: Domain Groups, Remote System Discovery, System Network Configuration Discovery

- ID: 56714
  - Name: Cobalt Strike
Adversary Emulation
How Adversary Emulation Works

• It takes a formal model of adversary behaviour
  – I.e. the tactics and groups from ATT&CK
• And carries out activities of that model
  – I.e. the techniques
• On systems of your network
  – Executing element: Agent
• An emulation consists of a series/group of activities
  – Aka Operation/Scenario/Campaign/Profile
  – Selected part of infrastructure = Application, system, network, etc.
• End result is a report/visualization (usually a web page)
Agents

- Used to gather Information
  - Vulnerabilities
  - System information
  - Sensible information (stuff that adversaries want to exfiltrate)

- And carrying out other activities
  - May be run persistently or uninstall after the emulation
  - Privilege level depends on deployment, i.e. root/admin or unprivileged user

- Combination with other tools
  - Import of vulnerability data from other tools, like Nmap
  - Post-exploitation tool together with pentest tools like Metasploit
Adversary Emulation Demo
Mitre Caldera
Critique

• ATT&CK as a general model for adversary behaviour
  – No all emulation tools use it, others may use their own model
  – If you want/need a specific model, check with the vendor
  – Better on the vulnerability side, CVE is almost universally accepted

• Import of vulnerability data from other tools limited
  – Like OpenVAS, OWASP ZAP, ...

• Security
  – Agents are Remote Access Trojans!
  – Deployment on production networks?

• Privacy protection (need we say more?)
  – This is vital (esp. under GDPR)
Adversary Emulation vs.

• **Penetration Tests**
  - Penetration tests are usually more limited in scope, i.e. finding vulnerabilities in one application or network
  - Adversary (the penetration tester) is not bound to tactics or techniques
  - Creativity is the distinguishing element

• **High-level tabletop exercises** *(e.g. CLAWS)*
  - Focuses on the procedural/human level of incident response
  - Blue/Purple team exercises can be carried out with (some) tools
  - However, they focus more on the technical level
  - Like: "Did the SOC notice a given technique/tactic?"
Finally

- Scans, detection, emulation do **not** make a network more secure!
- The real work is
  - **Closing the vulnerabilities**, and
  - **Changing operating procedures (i.e. human behaviour)**
- Which is as hard as before
- Besides that …
  - Campaign/Operation has to be planned carefully in advance
    - That’s work too!
  - Purchasing and maintaining a tool takes effort also
  - Planning and execution needs in-house cooperation
What have you learned?

- Adversary Emulation can be an additional tool for
  - Testing your detection mechanisms
  - Raising awareness
- Takes careful planning
- Start small, expand later - you will never be 100% perfect

What’s Next?

- Next module: *Forensics for Admins*
  - How to acquire forensic evidence on compromised systems
- Coming soon on GÉANT WP8
Thank you

Any questions?

Next Module: *Forensics for Admins*

*Coming soon:)*

www.geant.org
References:

- Mitre ATT&CK: https://attack.mitre.org/
- Meta Attack Language (MAL) (used by foreseeti)
  - https://mal-lang.org
  - https://github.com/mal-lang
  - https://docs.foreseeti.com/docs
- Pyramid of Pain: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- OVAL/SCAP, CVE, CVSS, CPE, ...
  https://oval.mitre.org/adoption/usecasesguide.html#vulnerability
Open Source Adversarial Emulation Tools

- InfectionMonkey (Guardicore)
  - https://www.guardicore.com/infectionmonkey/
  - https://github.com/guardicore/monkey
- Metta adversarial simulation tool (Uber)
  - https://github.com/uber-common/metta
- CALDERA (Mitre)
  - https://github.com/mitre/caldera
- AlphaSOC: FlightSIM tool for generating malicious network traffic
  - https://github.com/alphasoc/flightsim
- Red Canary: Atomic Red Team tests
  - https://github.com/redcanaryco/atomic-red-team
- Endgame: Red Team Automation (RTA) Scripts
  - https://github.com/endgameinc/RTA
Commercial Adversarial Emulation Tools

- SafeBreach
- foreseeeti: SecuriCAD
- AttackIQ
- Scythe
- XM Cyber: HaXM
- Randori
- Picus Security: Picus
- Cymulate
- CyCognito
- FireEye: Mandiant SIEM, enthält ex Verodin
- FireMon: Risk Analyzer
- Qualys: VMDR (Vulnerability Management, Detection, and Response) platform
Mitre STIX