—Senior security consultant

—Infrastructure assessments

—Red teaming and adversary emulation

—GPEN, GRID, GDAT

Jonas Bauters

✉️ jbauters@nviso.be

LinkedIn 🌐 www.linkedin.com/in/jonasbauters
Contents

The journey is more important than the destination

Our Approach

3

Red Teaming

2

Penetration Testing

1

Simulation & Emulation

4

TIBER

5

Purple Teaming

6
Penetration Testing

The start of our journey
What it isn’t

Penetration test

Vulnerability Assessment
- Host discovery
- Port & service enumeration
- Vulnerability identification

Exploitation
- Abuse the vulnerability
- Determine the business impact

Reporting
- Classification (High/Medium/Low)
- Description, business impact, reco
- Exploit chains
Should we abandon pentesting?

A traditional pentest still offers value

A traditional penetration test provides a report with:

- Context and scope
- Confirmed findings
- Realistic risk rating
- Recommendations
The need for adversary emulation

- Tactics, Techniques & Procedures
- Describe adversary activities
There is more

What a traditional pentest will not cover

Exposure to a **realistic, relevant** threat that is targeting your critical systems

On top of vulnerability identification, assess **detection capability**

Testing of the **human reaction**

Repeatable, structured process that provides **key areas for improvement**
Red Team Trifecta

This is where the Red Team comes in

Technology

Process

People

Pentest A

Pentest B

TTPs

Assess resilience

Improve resilience
Introducing Tactics, Techniques & Procedures

The Pyramid of Pain

Source: [http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html](http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html) by David Bianco
MITRE ATT&CK

A repository for TTPs

MITRE has developed the ATT&CK Matrix as a central repository for adversary TTPs.

It is used by both red and blue teams, which resulted in a lot of initiatives making use of the framework.

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>Applescript</td>
<td>bash_profile and bash</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Applescript</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Community Used Port</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>CMSTP</td>
<td>Accessibility Features</td>
<td>Accessibilty Features</td>
<td>BITS Jobs</td>
<td>Bash History</td>
<td>Application Window Discovery</td>
<td>Application Deployment Software</td>
<td>Automated Collection</td>
<td>Data Compressed</td>
<td>Communication Through Removable Media</td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Command-Line Interface</td>
<td>Account Manipulation</td>
<td>AppCert DLLs</td>
<td>Binary Padding</td>
<td>Bide Force</td>
<td>Browser Bookmark Discovery</td>
<td>Distributed Component Object Model</td>
<td>Clipboard Data</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Compiled HTML File</td>
<td>AppCert DLLs</td>
<td>AppCert DLLs</td>
<td>Bypass User Account Control</td>
<td>Credential Dumping</td>
<td>File and Directory Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data Staged</td>
<td>Data Transfer Size Limits</td>
<td>Custom Command and Control Protocol</td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Control Panel Items</td>
<td>Appinit DLLs</td>
<td>Application Shimming</td>
<td>CMSTP</td>
<td>Credentials in Files</td>
<td>Network Service Scanning</td>
<td>Logon Scripts</td>
<td>Data from Information Repositories</td>
<td>Exfiltration Over Alternative Protocol</td>
<td>Custom Cryptographic Protocol</td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>Dynamic Data Exchange</td>
<td>Application Shimming</td>
<td>Bypass User Account Control</td>
<td>Clear Command History</td>
<td>Credentials in Registry</td>
<td>Network Share Discovery</td>
<td>Pass the Hash</td>
<td>Data from Local System</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Data Encoding</td>
</tr>
<tr>
<td>Spearphishing via Service</td>
<td>Execution through API</td>
<td>Authentication Package</td>
<td>DLL Snatch Order Hijacking</td>
<td>Code Signing</td>
<td>Exploitation for Credential Access</td>
<td>Network Sniffing</td>
<td>Pass the Ticket</td>
<td>Data from Network Shared Drive</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Data Obfuscation</td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>Execution through Module Load</td>
<td>BITS Jobs</td>
<td>Dylib Hijacking</td>
<td>Compiled HTML File</td>
<td>Forced Authentication</td>
<td>Password Policy Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Data from Removable Media</td>
<td>Exfiltration Over Physical Medium</td>
<td>Domain Fronting</td>
</tr>
</tbody>
</table>

www.nviso.be  | 11
What does a realistic attack look like?

The Cyber Kill Chain™, created by Lockheed Martin in 2011, is a sequence of steps that describes how adversaries operate.
What does a realistic attack look like?

Cyber Kill Chain™ limitations

Even though it’s highly useful and has been widely adopted, there are some limitations.
The Unified Kill Chain (UKC)

Improving the Cyber Kill Chain™

Our Approach
Putting it all together

KEEPING OUR APPROACH TO OURSELVES

SHARING OUR APPROACH SO THE COMMUNITY CAN BENEFIT
Abstraction Levels

Emulating the adversary on multiple levels

- **Strategic**
  - Definition of flags/objectives
  - “Why”

- **Tactical**
  - Sequence of phases aimed to achieve strategic objectives
  - Grouping of related techniques
  - “What”

- **Operational**
  - Specific techniques & procedures
  - Execution and completion of tactical phases
  - “How”
Abstraction Levels

A metaphor

Operational

Tactical

Strategic
Mapping the adversary’s objectives to the Kill Chain

**Yellow Tier**
- Confidential data online
- External server or website compromise
- Access to internal network
- Credentials obtained via phishing

**Orange Tier**
- Local server admin
- Local workstation admin
- Domain Administrator

**Red Tier**
- Crown Jewel
- Sensitive Data
- Critical Asset

Initial Foothold (Compromised System) -> Pivoting -> Network Propagation (Internal Network) -> Access -> Action on Objectives (Critical Asset Access)
Strategic Level

Mapping the adversary’s objectives to the Kill Chain

Yellow Tier
- Confidential data online
- External server or website compromise
- Access to internal network
- Credentials obtained via phishing

Orange Tier
- Local server admin
- Local workstation admin
- Domain Administrator

Red Tier
- Crown Jewel
- Sensitive Data
- Critical Asset

Initial Foothold (Compromised System) → Pivoting → Network Propagation (Internal Network) → Access → Action on Objectives (Critical Asset Access)
Tactical Level

Mapping the adversary’s tactical phases to the Kill Chain

PRE-ATT&CK™

ATT&CK™

- Information Gathering
- Weakness Identification
- Build Capabilities
- Initial Access
- Privilege Escalation
- Lateral Movement
- Data Collection

- Initial Foothold (Compromised System)
- Pivoting
- Network Propagation (Internal Network)
- Access
- Action on Objectives (Critical Asset Access)
Operational Level

Mapping the adversary’s techniques to the Kill Chain

**Tactic:** Info Gathering
**Technique:** Active scanning

**Tactic:** Lateral Movement
**Technique:** Pass the hash

**Tactic:** Data Collection
**Technique:** Input Capture

**Initial Foothold** (Compromised System) ➔ **Pivoting** ➔ **Network Propagation** (Internal Network) ➔ **Access** ➔ **Action on Objectives** (Critical Asset Access)
Kill Chain Comparison

One environment is not like the other

**Company ABC**
- **Tactic**: Initial Access
- **Technique**: Hardware Add-on

**Company XYZ**
- **Tactic**: Initial Access
- **Technique**: Spear Phishing

---

**Tactic**: Credential Access
- **Technique**: LLMNR Poisoning
- **Technique**: Credential Dump

**Tactic**: Lateral Movement
- **Technique**: Pass-The-Hash

**Tactic**: Lateral Movement
- **Technique**: RDP

---

Local Admin
Detailed Kill Chain
Mapping findings to TTPs

**Tactic**
Initial Access

**Techniques**
- Hardware add-on
- Insufficient physical protection
- Lack of network access control

**Tactic**
Discovery

**Techniques**
- System discovery
- Service scanning
- Improper network segregation
- SMB signing disabled

**Tactic**
Credential Access

**Techniques**
- LLMNR poisoning
- Credential dump (SAM)
- Local name resolution enabled
- Admin privileges assigned to regular accounts

**Tactic**
Lateral Movement

**Techniques**
- Pass-the-hash

Orange-Tier objective reached:
- Local Admin on Server

www.nviso.be | 23
Simulation vs. Emulation

The devil is in the details
(Si|E)mulation

Does it even matter?

**Simulate** - verb [ T ] /ˈsɪm.jə.leɪt/

To produce something that is not real but has the appearance of being real.

**Emulate** - verb [ T ] /ˈem.jə.leɪt/

To behave in the same way as someone else.
Adversary (Si|E)mulation

It does matter

Emulation
— Based on threat intelligence
— TTPs of adversaries that will target you
— Based on a previous simulation

Simulation
— Based on the Red Team’s experience
— Based on environment at hand
— Based on global technique popularity

Impersonate
APT-28

Simulate an adversary that is not real
Adversary Emulation

Emulating a specific adversary's TTPs
Adversary Simulation

Simulating a threat by using the TTPs that work for that target/environment

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command And Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>CMSTP</td>
<td>Command-Line Interface</td>
<td>Exploit Public-Facing Application</td>
<td>Exploit for Client Execution</td>
<td>Exploit for Privilege Escalation</td>
<td>Extra Memory Injection</td>
<td>Extra Window Memory Injection</td>
<td>File System Permissions Weakness</td>
<td>Hooking</td>
<td>LLMNR/NET-NS Poisoning and Relay</td>
<td>Security Software Discovery</td>
</tr>
<tr>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit for Privilege Escalation</td>
</tr>
</tbody>
</table>
Emulate Adversary

- Threat-Intelligence Based Ethical Red Team
- “Classic” Red Team

Simulate Adversary

Remain undetected

YOUR QUADRANT IS BAD
AND YOU SHOULD FEEL BAD
Remain undetected

Emulate Adversary

Threat-Intelligence Based Ethical Red Team

“Classic” Red Team
TIBER
A European initiative to structure Red Teaming

- Require most important financial institutions to perform TIBER testing
- Guide institutions with procurement
- Follow-up on the testing together with White Team

“TIBER tests mimic potential attacks by real high level threat groups ...”
“... without the foreknowledge of the organisation’s defending Blue Team.”
TIBER

Process Overview

GTI | Preparation | Testing | Closure

- Generic Threat Intelligence
- Targets
- Threats
- Targeted Threat Intel Report
- Red Team Test Plan
- Red Team

Threat Intelligence
It doesn’t end here

It’s not just about offense

**Me:** *Discuss adversary emulation without including the blue team*

**The blue team:**

— So far, we’ve focused on the offensive side.

— Red Team goal: test detection capabilities, human aspect, process improvements.

— It’s time to take the blue team into account!
Remain undetected

Emulate Adversary

Threat-Intelligence Based Ethical Red Team

Threat-Intelligence Based Purple Team

Blue team co-op

“Classic” Red Team

Purple Simulation

Simulate Adversary

NOT SURE IF QUADRANT STARTING TO MAKE SENSE
OR TOO HUNGRY TO THINK STRAIGHT
Purple Team
Red Team vs Blue Team

Team work makes the dream work

COMMON GOAL

Improve security posture

Vulnerability Identification
Exploitation
Social Engineering

Implementing Controls
Security Monitoring
Incident Response

Source: SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
How it’s usually done

Red vs Blue

- Many vulnerabilities == Good job!
- Success is measured by # of failed controls
- Blue team failure == Red team success!
- No alerts? Preventive controls are working!
- Lots of alerts? Detection is working!
- Red team failure = Blue team success!

Different reporting hierarchy & different objectives result in red and blue not being aligned and a lack of incentive to help each other.

Source: SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
How it could be

What about some of the following actions?

- Share TTPs of new threat actors
- Help with vulnerability management and prioritize most critical issues
- Test Red Team techniques
- Share monitoring tactics, playbooks, and alerting

Source: SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
Purple Prerequisites

Purple teaming is the new red teaming, right?

- Central logging platform
- Endpoint visibility
- Network device logs
- Manpower (or girlpower)
The best of both worlds

An example approach

Threat-Intelligence Based Ethical Red Team

“Classic” Red Team

Periodic assessment

Replay & align

Red

Blue

Emulation

Continuous improvement
Tracking improvement

All about those metrics

MITRE ATT&CK Navigator

- Time to Initial foothold
- Network propagation
- Time to detection
- Prevented TTPs

- Detected
- Not Detected
- Logs Available
- Not Tested
“Adversary Emulation” is not the final destination. There are different flavours that can be valid options, depending on your goals and environment.

However, advanced attack simulation and emulation should be based on realistic TTPs, for which MITRE is (becoming) the de facto framework.
Thank You

Questions or Food?