# A semantic approach for describing Advanced Persistant Threat

A. Berady - G. Guette - M. Jaume - **V. Viet Triem Tong**

EPI CIDRE INRIA / CentraleSupelec / CNRS / Univ. Rennes 1
`valerie.viettriemtong@centralesupelec.fr`

Supsec Winter Workshop
January 2023

# APT : Advanced Persistent Threat

A term coined by Colonel Greg Rattray (US Air Force) in 2006 and popularized the NIST in 2011

*The Advanced Persistent Threat :*

1. *pursues its objectives repeatedly over an extended period of time ;*
2. *adapts to defenders' efforts to resist it ; and*
3. *is determined to maintain the level of interaction needed to execute its objectives.*

# Before 2011, the real knowledge of APTs remains confidential

When the term APT started to be used, the general public has heard about

- Moonlight Maze (1996) : targeting US military and government networks pointing to Russian Internet Service Providers in 1996
- Titan Rain (2003) series of attacks in the US since 2003 originated from China
- StuxNext (2010) uncovered in 2010 and thought to have been in development since at least 2005, widely understood to be a cyberweapon against Iran
- Operation Aurora (2010) series of cyber attacks originated from China targeting over 20 US companies

Technology

This article is more than **15 years old**

Titan Rain - how Chinese hackers targeted Whitehall

- Foreign Office among departments hit
- Military involvement suspected

Ed Pilkington in New Y… and Bobbie Johns…

Wed 5 Sep 2007 10.02 BST

China flexes muscles of its 'informationised' army

- Pentagon attack part of lon… networks
- Hacking incid… capabili…

120

Stuxnet worm heralds new era of global cyberwar

Attack aimed at Iran nuclear plant and recently revealed 2008 incident at US base show spread of cyber weapons

The Stuxnet … appeared to use contaminated hardware in an attempt to cripple Iran's nuclear programme. Photograph: Matthew Baker/…

The memory sticks were scattered in a washroom at a US military base in the … that was providing support for the Iran wa…

# More than 10 years later, if you want to study APT ?

## Few datasets [1]

- I won't talk about KDD99
- Unified Host and Network Dataset [2]
- DAPT 2020 [3]
- PWNJUTSU 2022 [4]

## Some un-structured reports

AptNotes https://github.com/aptnotes/
Operation Aurora, Malware Targeting Organizations in Ukraine

## Videos, tweet and other media

- TV5 Monde

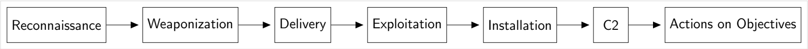
Few (No ?) details on the targeted architecture, the defense system, the precise attack scenario

# First Step : Global overview

*Lifecycle of an Advanced Persistant Threa*t

# APT Lifecycle : *Cyber Kill Chain* Lockheed Martin in 2011

- Linear model focusing on the initial compromise
- Cannot describe long-term attacks

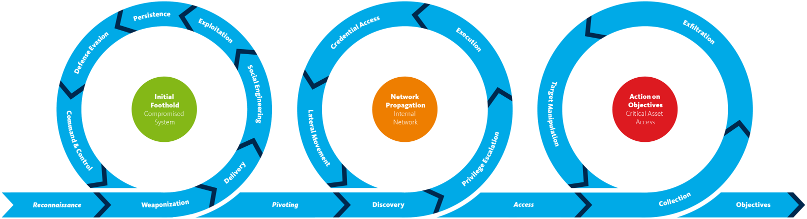


Reconnaissance → Weaponization → Delivery → Exploitation → Installation → C2 → Actions on Objectives

# ATP-Life-cycle : *Kill chains models*

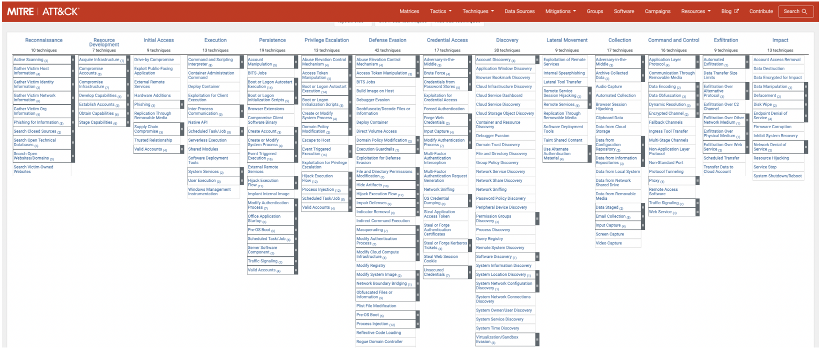
Pols in 2017 *Unified Kill Chain*

- introduces the notion of repetitiveness of technical actions
- introduces the notion of phases of APT
- does not consider the potential regression of the attacker.



# Tactics of the Attack matrix

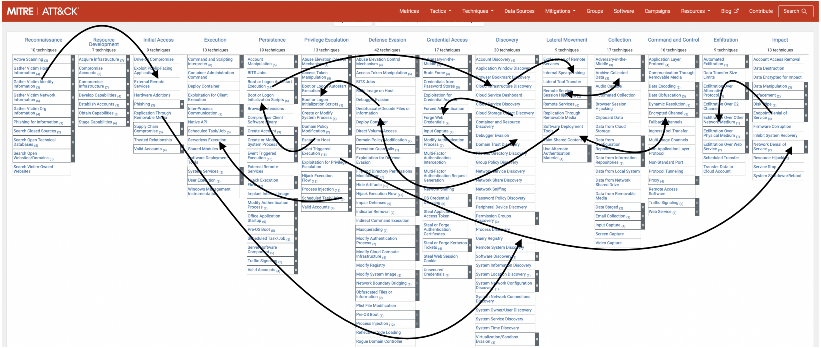
MITRE ATT&CK in 2013 a knowledge base of TTPs.



| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 techniques | 7 techniques | 9 techniques | 13 techniques | 19 techniques | 13 techniques | 42 techniques | 17 techniques | 30 techniques | 9 techniques | 17 techniques | 16 techniques | 9 techniques | 13 techniques |
| Active Scanning (3) | Acquire Infrastructure (7) | Drive-by Compromise | Command and Scripting Interpreter (8) | Account Manipulation (5) | Abuse Elevation Control Mechanism (4) | Abuse Elevation Control Mechanism (4) | Adversary-in-the-Middle (3) | Account Discovery (4) | Exploitation of Remote Services | Adversary-in-the-Middle (3) | Application Layer Protocol (4) | Automated Exfiltration (1) | Account Access Removal |
| Gather Victim Host Information (4) | Compromise Accounts (3) | Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation (5) | Access Token Manipulation (5) | Brute Force (4) | Application Window Discovery | Internal Spearphishing | Archive Collected Data (3) | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| Gather Victim Identity Information (3) | Compromise Infrastructure (7) | External Remote Services | Deploy Container | Boot or Logon Autostart Execution (14) | Boot or Logon Autostart Execution (14) | BITS Jobs | Credentials from Password Stores (5) | Browser Bookmark Discovery | Lateral Tool Transfer | Audio Capture | Data Encoding (2) | Exfiltration Over Alternative Protocol (3) | Data Encrypted for Impact |
| Gather Victim Network Information (6) | Develop Capabilities (4) | Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts (5) | Boot or Logon Initialization Scripts (5) | Build Image on Host | Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking (2) | Automated Collection | Data Obfuscation (3) | Exfiltration Over C2 Channel | Data Manipulation (3) |
| Gather Victim Org Information (4) | Establish Accounts (3) | Phishing (3) | Inter-Process Communication (3) | Browser Extensions | Create or Modify System Process (4) | Debugger Evasion | Forced Authentication | Cloud Service Dashboard | Remote Services (6) | Browser Session Hijacking | Dynamic Resolution (3) | Exfiltration Over Other Network Medium (1) | Defacement (2) |
| Phishing for Information (3) | Obtain Capabilities (6) | Replication Through Removable Media | Native API | Compromise Client Software Binary | Domain Policy Modification (2) | Deobfuscate/Decode Files or Information | Forge Web Credentials (2) | Cloud Service Discovery | Replication Through Removable Media | Clipboard Data | Encrypted Channel (2) | Exfiltration Over Physical Medium (1) | Disk Wipe (2) |
| Search Closed Sources (2) | Stage Capabilities (6) | Supply Chain Compromise (3) | Scheduled Task/Job (5) | Create Account (3) | Escape to Host | Deploy Container | Input Capture (4) | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage | Fallback Channels | Exfiltration Over Web Service (2) | Endpoint Denial of Service (4) |
| Search Open Technical Databases (5) | | Trusted Relationship | Serverless Execution | Create or Modify System Process (4) | Event Triggered Execution (16) | Direct Volume Access | Modify Authentication Process (7) | Container and Resource Discovery | Taint Shared Content | Data from Configuration Repository (2) | Ingress Tool Transfer | Scheduled Transfer | Firmware Corruption |
| Search Open Websites/Domains (3) | | Valid Accounts (4) | Shared Modules | Event Triggered Execution (16) | Exploitation for Privilege Escalation | Domain Policy Modification (2) | Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate Authentication Material (4) | Data from Information Repositories (3) | Multi-Stage Channels | Transfer Data to Cloud Account | Inhibit System Recovery |
| Search Victim-Owned Websites | | | Software Deployment Tools | External Remote Services | Hijack Execution Flow (12) | Execution Guardrails (1) | Multi-Factor Authentication Request Generation | Domain Trust Discovery | | Data from Local System | Non-Application Layer Protocol | | Network Denial of Service (2) |
| | | | System Services (2) | Hijack Execution Flow (12) | Process Injection (12) | Exploitation for Defense Evasion | Network Sniffing | File and Directory Discovery | | Data from Network Shared Drive | Non-Standard Port | | Resource Hijacking |
| | | | User Execution (3) | Implant Internal Image | Scheduled Task/Job (5) | File and Directory Permissions Modification (2) | OS Credential Dumping (8) | Group Policy Discovery | | Data from Removable Media | Protocol Tunneling | | Service Stop |
| | | | Windows Management Instrumentation | Modify Authentication Process (7) | Valid Accounts (4) | Hide Artifacts (10) | Steal Application Access Token | Network Service Discovery | | Data Staged (2) | Proxy (4) | | System Shutdown/Reboot |
| | | | | Office Application Startup (6) | | Hijack Execution Flow (12) | Steal or Forge Authentication Certificates | Network Share Discovery | | Email Collection (3) | Remote Access Software | | |
| | | | | Pre-OS Boot (5) | | Impair Defenses (9) | Steal or Forge Kerberos Tickets (4) | Network Sniffing | | Input Capture (4) | Traffic Signaling (2) | | |
| | | | | Scheduled Task/Job (5) | | Indicator Removal (9) | Steal Web Session Cookie | Password Policy Discovery | | Screen Capture | Web Service (3) | | |
| | | | | Server Software Component (5) | | Indirect Command Execution | Unsecured Credentials (7) | Peripheral Device Discovery | | Video Capture | | | |
| | | | | Traffic Signaling (2) | | Masquerading (7) | | Permission Groups Discovery (3) | | | | | |
| | | | | Valid Accounts (4) | | Modify Authentication Process (7) | | Process Discovery | | | | | |
| | | | | | | Modify Cloud Compute Infrastructure (4) | | Query Registry | | | | | |
| | | | | | | Modify Registry | | Remote System Discovery | | | | | |
| | | | | | | Modify System Image (2) | | Software Discovery (1) | | | | | |
| | | | | | | Network Boundary Bridging (1) | | System Information Discovery | | | | | |
| | | | | | | Obfuscated Files or Information (9) | | System Location Discovery (1) | | | | | |
| | | | | | | Plist File Modification | | System Network Configuration Discovery (1) | | | | | |
| | | | | | | Pre-OS Boot (5) | | System Network Connections Discovery | | | | | |
| | | | | | | Process Injection (12) | | System Owner/User Discovery | | | | | |
| | | | | | | Reflective Code Loading | | System Service Discovery | | | | | |
| | | | | | | Rogue Domain Controller | | System Time Discovery | | | | | |
| | | | | | | | | Virtualization/Sandbox Evasion (3) | | | | | |

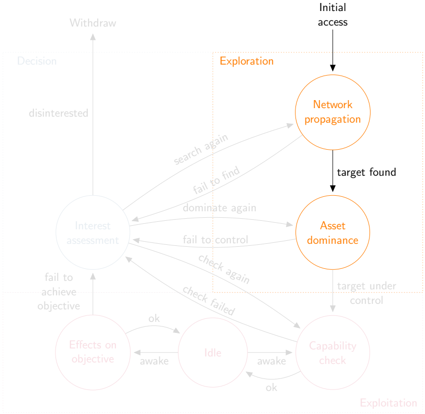
# Tactics of the Attack matrix

*MITRE ATT&CK* is not a model per se but it deepens the notion of phase of an attack without highlighting their ordering

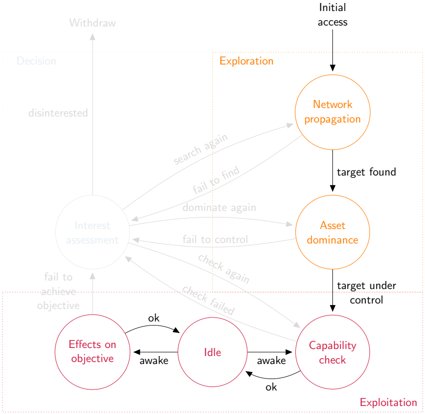


| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 techniques | 7 techniques | 9 techniques | 13 techniques | 19 techniques | 13 techniques | 42 techniques | 17 techniques | 30 techniques | 9 techniques | 17 techniques | 16 techniques | 9 techniques | 13 techniques |
| Active Scanning (3) | Acquire Infrastructure (7) | Drive-by Compromise | Command and Scripting Interpreter (8) | Account Manipulation (5) | Abuse Elevation Control Mechanism (4) | Abuse Elevation Control Mechanism (4) | Adversary-in-the-Middle (3) | Account Discovery (4) | Exploitation of Remote Services | Adversary-in-the-Middle (3) | Application Layer Protocol (4) | Automated Exfiltration (1) | Account Access Removal |
| Gather Victim Host Information (4) | Compromise Accounts (3) | Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation (5) | Access Token Manipulation (5) | Brute Force (4) | Application Window Discovery | Internal Spearphishing | Archive Collected Data (3) | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| Gather Victim Identity Information (3) | Compromise Infrastructure (7) | External Remote Services | Deploy Container | Boot or Logon Autostart Execution (14) | Boot or Logon Autostart Execution (14) | BITS Jobs | Credentials from Password Stores (5) | Browser Bookmark Discovery | Lateral Tool Transfer | Audio Capture | Data Encoding (2) | Exfiltration Over Alternative Protocol (3) | Data Encrypted for Impact |
| Gather Victim Network Information (6) | Develop Capabilities (4) | Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts (5) | Boot or Logon Initialization Scripts (5) | Build Image on Host | Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking (2) | Automated Collection | Data Obfuscation (3) | Exfiltration Over C2 Channel | Data Manipulation (3) |
| Gather Victim Org Information (4) | Establish Accounts (3) | Phishing (3) | Inter-Process Communication (3) | Browser Extensions | Create or Modify System Process (4) | Debugger Evasion | Forced Authentication | Cloud Service Dashboard | Remote Services (6) | Browser Session Hijacking | Dynamic Resolution (3) | Exfiltration Over Other Network Medium (1) | Defacement (2) |
| Phishing for Information (3) | Obtain Capabilities (6) | Replication Through Removable Media | Native API | Compromise Client Software Binary | Domain Policy Modification (2) | Deobfuscate/Decode Files or Information | Forge Web Credentials (2) | Cloud Service Discovery | Replication Through Removable Media | Clipboard Data | Encrypted Channel (2) | Exfiltration Over Physical Medium (1) | Disk Wipe (2) |
| Search Closed Sources (2) | Stage Capabilities (6) | Supply Chain Compromise (3) | Scheduled Task/Job (5) | Create Account (3) | Escape to Host | Deploy Container | Input Capture (4) | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage | Fallback Channels | Exfiltration Over Web Service (2) | Endpoint Denial of Service (4) |
| Search Open Technical Databases (5) |  | Trusted Relationship | Serverless Execution | Create or Modify System Process (4) | Event Triggered Execution (16) | Direct Volume Access | Modify Authentication Process (7) | Container and Resource Discovery | Taint Shared Content | Data from Configuration Repository (2) | Ingress Tool Transfer | Scheduled Transfer | Firmware Corruption |
| Search Open Websites/Domains (3) |  | Valid Accounts (4) | Shared Modules | Event Triggered Execution (16) | Exploitation for Privilege Escalation | Domain Policy Modification (2) | Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate Authentication Material (4) | Data from Information Repositories (3) | Multi-Stage Channels | Transfer Data to Cloud Account | Inhibit System Recovery |
| Search Victim-Owned Websites |  |  | Software Deployment Tools | External Remote Services | Hijack Execution Flow (12) | Execution Guardrails (1) | Multi-Factor Authentication Request Generation | Domain Trust Discovery |  | Data from Local System | Non-Application Layer Protocol |  | Network Denial of Service (2) |
|  |  |  | System Services (2) | Hijack Execution Flow (12) | Process Injection (12) | Exploitation for Defense Evasion | Network Sniffing | File and Directory Discovery |  | Data from Network Shared Drive | Non-Standard Port |  | Resource Hijacking |
|  |  |  | User Execution (3) | Implant Internal Image | Scheduled Task/Job (5) | File and Directory Permissions Modification (2) | OS Credential Dumping (8) | Group Policy Discovery |  | Data from Removable Media | Protocol Tunneling |  | Service Stop |
|  |  |  | Windows Management Instrumentation | Modify Authentication Process (7) | Valid Accounts (4) | Hide Artifacts (10) | Steal Application Access Token | Network Service Discovery |  | Data Staged (2) | Proxy (4) |  | System Shutdown/Reboot |
|  |  |  |  | Office Application Startup (6) |  | Hijack Execution Flow (12) | Steal or Forge Authentication Certificates | Network Share Discovery |  | Email Collection (3) | Remote Access Software |  |  |
|  |  |  |  | Pre-OS Boot (5) |  | Impair Defenses (9) | Steal or Forge Kerberos Tickets (4) | Network Sniffing |  | Input Capture (4) | Traffic Signaling (2) |  |  |
|  |  |  |  | Scheduled Task/Job (5) |  | Indicator Removal (9) | Steal Web Session Cookie | Password Policy Discovery |  | Screen Capture | Web Service (3) |  |  |
|  |  |  |  | Server Software Component (5) |  | Indirect Command Execution | Unsecured Credentials (7) | Peripheral Device Discovery |  | Video Capture |  |  |  |
|  |  |  |  | Traffic Signaling (2) |  | Masquerading (7) |  | Permission Groups Discovery (3) |  |  |  |  |  |
|  |  |  |  | Valid Accounts (4) |  | Modify Authentication Process (7) |  | Process Discovery |  |  |  |  |  |
|  |  |  |  |  |  | Modify Cloud Compute Infrastructure (4) |  | Query Registry |  |  |  |  |  |
|  |  |  |  |  |  | Modify Registry |  | Remote System Discovery |  |  |  |  |  |
|  |  |  |  |  |  | Modify System Image (2) |  | Software Discovery (1) |  |  |  |  |  |
|  |  |  |  |  |  | Network Boundary Bridging (1) |  | System Information Discovery |  |  |  |  |  |
|  |  |  |  |  |  | Obfuscated Files or Information (9) |  | System Location Discovery (1) |  |  |  |  |  |
|  |  |  |  |  |  | Plist File Modification |  | System Network Configuration Discovery (1) |  |  |  |  |  |
|  |  |  |  |  |  | Pre-OS Boot (5) |  | System Network Connections Discovery |  |  |  |  |  |
|  |  |  |  |  |  | Process Injection (12) |  | System Owner/User Discovery |  |  |  |  |  |
|  |  |  |  |  |  | Reflective Code Loading |  | System Service Discovery |  |  |  |  |  |
|  |  |  |  |  |  | Rogue Domain Controller |  | System Time Discovery |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Virtualization/Sandbox Evasion (3) |  |  |  |  |  |

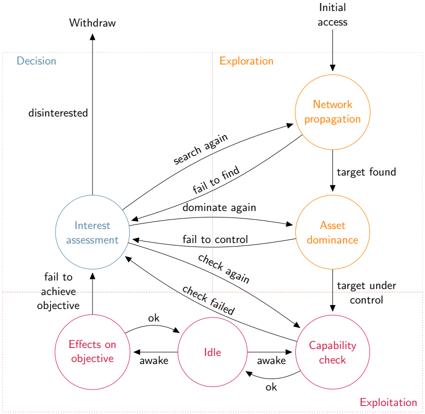
# Modeling the Operational Phases of APT Campaigns [5]



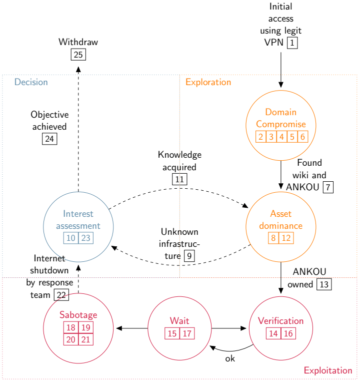
# Modeling the Operational Phases of APT Campaigns [5]



# Modeling the Operational Phases of APT Campaigns [5]



# Instantiation by the incident of TV5 Monde



Initial access using legit VPN 1

Withdraw 25

Decision

Exploration

Domain Compromise 2 3 4 5 6

Objective achieved 24

Knowledge acquired 11

Found wiki and ANKOU 7

Interest assessment 10 23

Asset dominance 8 12

Unknown infrastructure 9

Internet shutdown by response team 22

ANKOU owned 13

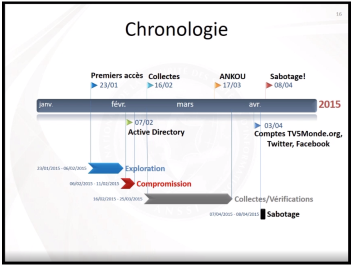
Sabotage 18 19 20 21

Wait 15 17

Verification 14 16

ok

Exploitation



16

Chronologie

Suppose that the community agrees on a generic model to represent an APT

but we still lack data..

varied, representative, up-to-date and above all accurate data

# PWNJUTSU project

PWNJUTSU

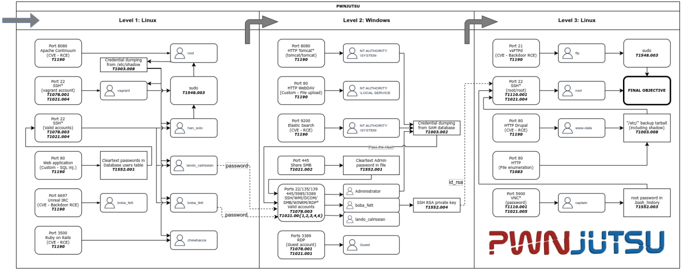
- Project funded and supported by IRSN BCyP
- 22 professional attackers attacks on a dedicated architecture
- New available dataset !

## Publication

Aimad Berady, Mathieu Jaume, Valérie Viet Triem Tong et Gilles Guette : **PWNJUTSU: A Dataset and a Semantics-Driven Approach to Retrace Attack Campaigns**.
*IEEE Transactions on Network and Service Management (TNSM), Special Issue on Recent Advances in Network Security Management*, 2022.

# PWNJUTSU Project overview

- 3 machines (Windows and Linux) : $M_1 \rightarrow M_2 \rightarrow M_3$
- mandatory checkpoints with *flags* to recover
- Several attack paths
- Vulnerabilities easy to exploit, so that the experimentation is focused on propagation in the network.



PWNJUTSU

Level 1: Linux

Port 8080
Apache Continuum
(CVE - RCE)
***T1190***

root

Credential dumping
from /etc/shadow
***T1003.008***

Port 22
SSH*
(vagrant account)
***T1078.001***
***T1021.004***

vagrant

sudo
***T1548.003***

Port 22
SSH*
(Valid accounts)
***T1078.003***
***T1021.004***

han_solo

Port 80
Web application
(Custom - SQL inj.)
***T1190***

Cleartext passwords in
Database users table
***T1552.001***

lando_calrissian

password

Port 6697
Unreal IRC
(CVE - Backdoor RCE)
***T1190***

boba_fett

boba_fett

password

Port 3500
Ruby on Rails
(CVE - RCE)
***T1190***

chewbacca

Level 2: Windows

Port 8080
HTTP Tomcat*
(tomcat/tomcat)
***T1190***

NT AUTHORITY
\SYSTEM

Port 80
HTTP WebDAV
(Custom - File upload)
***T1190***

NT AUTHORITY
\LOCAL SERVICE

Port 9200
Elastic Search
(CVE - RCE)
***T1190***

NT AUTHORITY
\SYSTEM

Credential dumping
from SAM database
***T1003.002***

*Pass-the-Hash*

Port 445
Share SMB
***T1021.002***

Cleartext Admin
password in file
***T1552.001***

Ports 22/135/139
445/5985/3389
SSH/WMI/DCOM/
SMB/WINRM/RDP*
Valid accounts
***T1078.003***
***T1021.00{1,2,3,4,6}***

Administrator

boba_fett

lando_calrissian

SSH RSA private key
***T1552.004***

id_rsa

Ports 3389
RDP
(Guest account)
***T1078.001***
***T1021.001***

Guest

Level 3: Linux

Port 21
vsFTPd
(CVE - Backdoor RCE)
***T1190***

ftp

sudo
***T1548.003***

Port 22
SSH*
(root/root)
***T1110.001***
***T1021.004***

root

FINAL OBJECTIVE

Port 80
HTTP Drupal
(CVE - RCE)
***T1190***

www-data

"/etc/" backup tarball
(including shadow)
***T1003.008***

Port 80
HTTP
(File enumeration)
***T1083***

Port 5900
VNC*
(password)
***T1110.001***
***T1021.005***

captain

root password in
.bash_history
***T1552.003***

PWNJUTSU

# PWNJUTSU Project – Overview

- Dedicated Instances for each participant.
- Probes on operating systems and verbose logs
- Continuous capture of network flows
- Supervision by a SIEM.

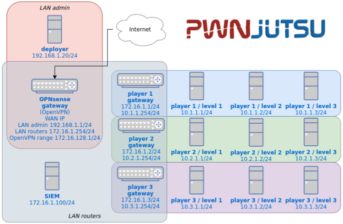


Figure – PWNJUTSU infrastructure

# PWNJUTSU Project – Participants

YES WE HACK

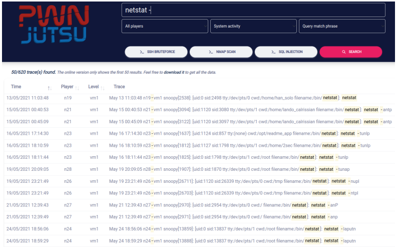
- 22 experts from the TOP100 of YesWeHack experts
- 9 nationalities
- Progressive and attractive financial rewards
- Typical participant profile :
  - 25-35 years old (63%) ;
  - Bachelor's/Master's level degree (91%) ;
  - Certified in "ethical hacking". (64%) ;
  - Self-trained offensive security expert(100%).

# PWNJUTSU dataset

https://pwnjutsu.irisa.fr

a raw dataset

- 16 million system events
- 172 GB of network traffic
- a search engine



netstat -

All players | System activity | Query match phrase

***50/620 trace(s) found.*** *The online version only shows the first 50 results. Feel free to* ***download it*** *to get all the data.*

| Time | Player | Level | Trace |
|---|---|---|---|
| 13/05/2021 11:03:48 | n19 | vm1 | May 13 11:03:48 n19-vm1 snoopy[2538]: [uid:0 sid:2498 tty:/dev/pts/0 cwd:/home/han_solo filename:/bin/netstat]: netstat |
| 15/05/2021 00:40:53 | n21 | vm1 | May 15 00:40:53 n21-vm1 snoopy[3094]: [uid:1120 sid:3080 tty:/dev/pts/1 cwd:/home/lando_calrissian filename:/bin/netstat]: netstat -antp |
| 15/05/2021 00:45:09 | n21 | vm1 | May 15 00:45:09 n21-vm1 snoopy[3122]: [uid:1120 sid:3097 tty:/dev/pts/1 cwd:/home/lando_calrissian filename:/bin/netstat]: netstat -antp |
| 16/05/2021 17:14:30 | n23 | vm1 | May 16 17:14:30 n23-vm1 snoopy[1637]: [uid:1124 sid:857 tty:(none) cwd:/opt/readme_app filename:/bin/netstat]: netstat -tunlp |
| 16/05/2021 18:10:59 | n23 | vm1 | May 16 18:10:59 n23-vm1 snoopy[1812]: [uid:1127 sid:1798 tty:/dev/pts/1 cwd:/home/2sec filename:/bin/netstat]: netstat -tunlp |
| 16/05/2021 18:11:44 | n23 | vm1 | May 16 18:11:44 n23-vm1 snoopy[1825]: [uid:0 sid:1798 tty:/dev/pts/1 cwd:/root filename:/bin/netstat]: netstat -tunlp |
| 19/05/2021 20:09:05 | n28 | vm1 | May 19 20:09:05 n28-vm1 snoopy[1907]: [uid:0 sid:1870 tty:/dev/pts/0 cwd:/root filename:/bin/netstat]: netstat -tunap |
| 19/05/2021 23:21:49 | n26 | vm1 | May 19 23:21:49 n26-vm1 snoopy[26711]: [uid:1120 sid:26339 tty:/dev/pts/0 cwd:/tmp filename:/bin/netstat]: netstat -nupl |
| 19/05/2021 23:21:49 | n26 | vm1 | May 19 23:21:49 n26-vm1 snoopy[26703]: [uid:1120 sid:26339 tty:/dev/pts/0 cwd:/tmp filename:/bin/netstat]: netstat -ntpl |
| 21/05/2021 12:39:43 | n27 | vm1 | May 21 12:39:43 n27-vm1 snoopy[2970]: [uid:0 sid:2954 tty:/dev/pts/0 cwd:/ filename:/bin/netstat]: netstat -anP |
| 21/05/2021 12:39:49 | n27 | vm1 | May 21 12:39:49 n27-vm1 snoopy[2971]: [uid:0 sid:2954 tty:/dev/pts/0 cwd:/ filename:/bin/netstat]: netstat -anp |
| 24/05/2021 18:56:06 | n24 | vm1 | May 24 18:56:06 n24-vm1 snoopy[13859]: [uid:0 sid:13837 tty:/dev/pts/1 cwd:/root filename:/bin/netstat]: netstat -laputn |
| 24/05/2021 18:59:29 | n24 | vm1 | May 24 18:59:29 n24-vm1 snoopy[13888]: [uid:0 sid:13837 tty:/dev/pts/1 cwd:/root filename:/bin/netstat]: netstat -laputn |

Here we have data

but how to present them ?

we need a way to detail the whole scenario
and each particular attack progression

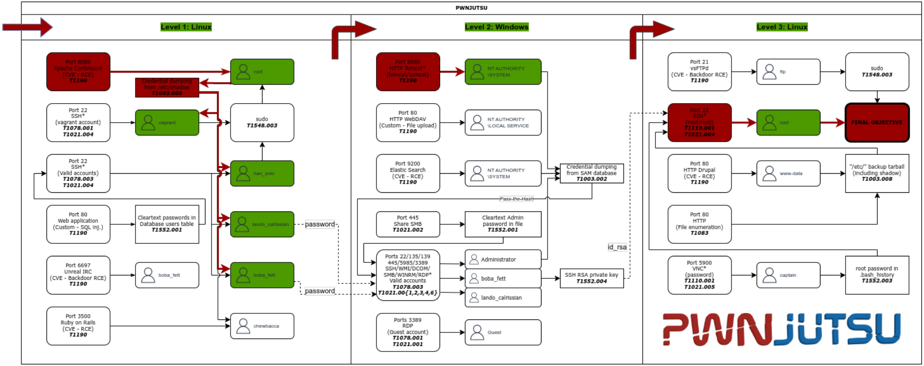
# Attacker's report

## Extract from P12 report

1. scan nmap (1000 ports) through the VPN.
2. Discovery of several services.
3. Recover banners and discover the continuum application.
4. Launched a bruteforce on the SSH port (without success and not very functional).
5. Search for public vulnerabilities on continuum.
6. Usage of Metasploit module to successfully exploit the continuum vulnerability.
7. I obtained a shell and fast environment of the machine.

Informel report where some element are missing, attacker's perspective only

# P12 progression



PWNJUTSU

Level 1: Linux

Port 8080
Apache Continuum
(CVE - RCE)
*T1190*

root

Credential dumping
from /etc/shadow
*T1003.008*

Port 22
SSH*
(vagrant account)
*T1078.001*
*T1021.004*

vagrant

sudo
*T1548.003*

Port 22
SSH*
(Valid accounts)
*T1078.003*
*T1021.004*

han_solo

Port 80
Web application
(Custom - SQL Inj.)
*T1190*

Cleartext passwords in
Database users table
*T1552.001*

lando_calrissian

password

Port 6697
Unreal IRC
(CVE - Backdoor RCE)
*T1190*

boba_fett

boba_fett

password

Port 3500
Ruby on Rails
(CVE - RCE)
*T1190*

chewbacca

Level 2: Windows

Port 8080
HTTP Tomcat*
(tomcat/tomcat)
*T1190*

NT AUTHORITY
\SYSTEM

Port 80
HTTP WebDAV
(Custom - File upload)
*T1190*

NT AUTHORITY
\LOCAL SERVICE

Port 9200
Elastic Search
(CVE - RCE)
*T1190*

NT AUTHORITY
\SYSTEM

Credential dumping
from SAM database
*T1003.002*

*Pass-the-Hash*

Port 445
Share SMB
*T1021.002*

Cleartext Admin
password in file
*T1552.001*

Ports 22/135/139
445/5985/3389
SSH/WMI/DCOM/
SMB/WINRM/RDP*
Valid accounts
*T1078.003*
*T1021.00{1,2,3,4,6}*

Administrator

boba_fett

lando_calrissian

SSH RSA private key
*T1552.004*

id_rsa

Ports 3389
RDP
(Guest account)
*T1078.001*
*T1021.001*

Guest

Level 3: Linux

Port 21
vsFTPd
(CVE - Backdoor RCE)
*T1190*

ftp

sudo
*T1548.003*

Port 22
SSH*
(root/root)
*T1110.001*
*T1021.004*

root

FINAL OBJECTIVE

Port 80
HTTP Drupal
(CVE - RCE)
*T1190*

www-data

"/etc/" backup tarball
(including shadow)
*T1003.008*

Port 80
HTTP
(File enumeration)
*T1083*

Port 5900
VNC*
(password)
*T1110.001*
*T1021.005*

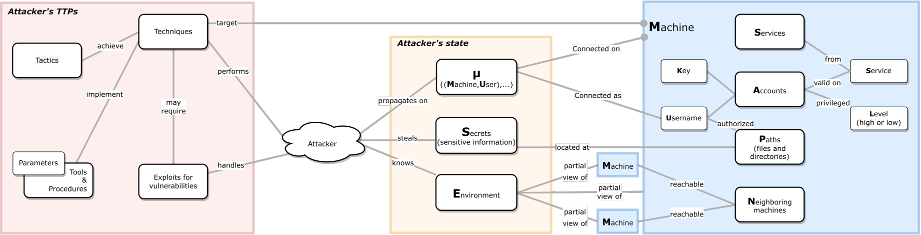
captain

root password in
.bash_history
*T1552.003*

PWNJUTSU

This progression has been manually inferred and represented.

# An attacker centric model to retrace attack campaign



An attacker state

- $\mu$ an attack position (machine, user)
- $\mathcal{S}$ the recovered secrets
- $\mathcal{E}$ a partial view of the targeted system

A targeted system is a set of machines. A machine $\mathbf{m}$

- $\mathbb{S}_{\mathbf{m}}$ : services
- $\mathbb{P}_{\mathbf{m}}$ : some files
- $\mathbb{A}_{\mathbf{m}}$ : accounts
- $\mathbb{N}_{\mathbf{m}}$ : a neighboring

# Progression of an attacker

A complete attack campaign is a sequence of attacker states representing the evolution of his control of the target.

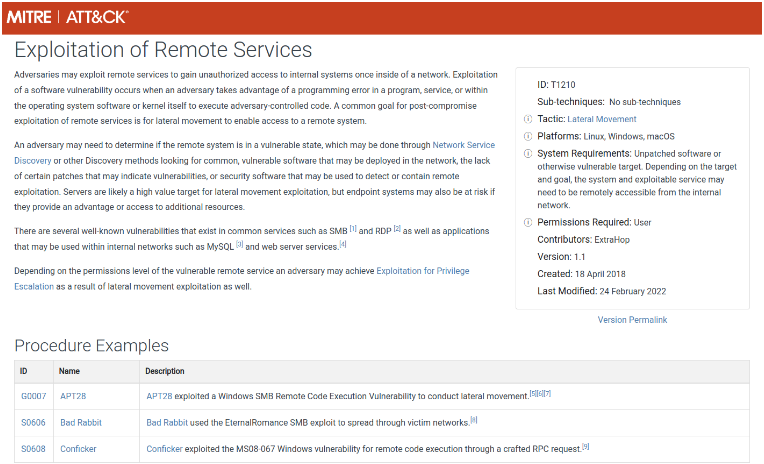
The attacker moves from one state to another by applying an attack technique.

$$(\mu_i, \mathcal{S}_i, \mathcal{E}_i) \xhookrightarrow{\mathbf{t}(\mathit{params})} (\mu_{i+1}, \mathcal{S}_{i+1}, \mathcal{E}_{i+1})$$

The attack techniques are those defined by the MITRE attack

These techniques are still defined in nature language and do not have a precise semantic.

# MITRE ATT&CK – T1210



MITRE | ATT&CK®

## Exploitation of Remote Services

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine if the remote system is in a vulnerable state, which may be done through Network Service Discovery or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

There are several well-known vulnerabilities that exist in common services such as SMB [1] and RDP [2] as well as applications that may be used within internal networks such as MySQL [3] and web server services.[4]

Depending on the permissions level of the vulnerable remote service an adversary may achieve Exploitation for Privilege Escalation as a result of lateral movement exploitation as well.

ID: T1210

Sub-techniques: No sub-techniques

ⓘ Tactic: Lateral Movement

ⓘ Platforms: Linux, Windows, macOS

ⓘ System Requirements: Unpatched software or otherwise vulnerable target. Depending on the target and goal, the system and exploitable service may need to be remotely accessible from the internal network.

ⓘ Permissions Required: User

Contributors: ExtraHop

Version: 1.1

Created: 18 April 2018

Last Modified: 24 February 2022

Version Permalink

### Procedure Examples

| ID | Name | Description |
|---|---|---|
| G0007 | APT28 | APT28 exploited a Windows SMB Remote Code Execution Vulnerability to conduct lateral movement.[5][6][7] |
| S0606 | Bad Rabbit | Bad Rabbit used the EternalRomance SMB exploit to spread through victim networks.[8] |
| S0608 | Conficker | Conficker exploited the MS08-067 Windows vulnerability for remote code execution through a crafted RPC request.[9] |

# A semantic for the technique *Exploitation of Remote Services*

| | |
|---|---|
| Technic | $T_{1210}$ : *Exploitation of Remote Services* |
| Tactic | *Lateral movement* |
| Description | Gain access to a machine by remotely exploiting a vulnerability using $x$ exploit on an exposed network service s. |
| Parameters | $\mathbf{m}$, $\mathbf{u}$, $\mathbf{m}'$, s, $x$ |
| Préconditions | $(\mathbf{m},\mathbf{u}) \in \mu$,<br>$\mathbf{m}' \in \lfloor \mathbb{N}_{\mathbf{m}} \rfloor_{\mathcal{E}}$,<br>$\mathrm{s} \in \lfloor \mathbb{S}_{\mathbf{m}'} \rfloor_{\mathcal{E}}$ et<br>$x \in$ *Exploits*(s) |
| Transition | $(\mu,\mathcal{S},\mathcal{E}) \hookrightarrow (\mu',\mathcal{S},\mathcal{E})$<br>where $\mu' = \mu \cup \{(\mathbf{m}',\mathbf{u}')\}$<br>with $(\mathbf{u}',\mathrm{s},\mathrm{k},\ell) \in \mathbb{A}_{\mathbf{m}'}$ |
| Variants | Authenticated vulnerabilities use the additional parameters $\mathbf{u}''$ and $\mathrm{k}''$ such as $(\mathbf{u}'',\mathrm{s},\mathrm{k}'',\ell'') \in \lfloor \mathbb{A}_{\mathbf{m}'} \rfloor_{\mathcal{E}}$ |

# A semantic for the technique *Network Service Scanning* T1046

| | |
|---|---|
| TECHNIQUE | $T_{1046}$ : *Network Service Scanning* |
| TACTIQUE | *Discovery* |
| DESCRIPTION | Discover all network services of a remote machine $\mathbf{m}'$ by browsing the namespace of network ports $\Delta \subseteq \{0, \cdots, 65535\}$. |
| PARAMÈTRES | $\mathbf{m}$, $\mathbf{u}$, $\mathbf{m}'$, $\Delta$ |
| PRÉCONDITIONS | $(\mathbf{m}, \mathbf{u}) \in \mu$,<br>$\mathbf{m}' \in \lfloor \mathbb{N}_{\mathbf{m}} \rfloor_{\mathcal{E}}$ |
| TRANSITION | $(\mu, \mathcal{S}, \mathcal{E}) \hookrightarrow (\mu, \mathcal{S}, \mathcal{E}')$ with<br>$\mathcal{E}' = \mathcal{E}\,[\mathbf{m}' \leftarrow (\lfloor \mathbb{S}_{\mathbf{m}'} \rfloor_{\mathcal{E}} \cup \{\mathsf{s}(\mathrm{port} : i) \mid i \in \Delta\}, \lfloor \mathbb{P}_{\mathbf{m}'} \rfloor_{\mathcal{E}}, \lfloor \mathbb{A}_{\mathbf{m}'} \rfloor_{\mathcal{E}}, \lfloor \mathbb{N}_{\mathbf{m}'} \rfloor_{\mathcal{E}})]$ |

# Attack technics semantics

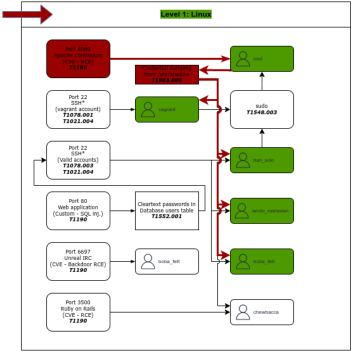
In [4] we detail the specification of 13 techniques, which satisfy 5 tactics :

- **Lateral Movement** : horizontal movement in the network (same user, different machine) ;
- **Credential Access** : collection of credentials ;
- **Privilege Escalation** : vertical movement in the network (different user, same machine) ;
- **Discovery** : discovery of the technical environment ;
- **Persistence** : implementation of a permanent remote access mechanism.

# P12 progression (reminder)

## Extract from P12 report

1. scan nmap (1000 ports) through the VPN.
2. Discovery of several services.
3. Recover banners and discover the continuum application.
4. Launched a bruteforce on the SSH port (without success and not very functional).
5. Search for public vulnerabilities on continuum.
6. Usage of Metasploit module to successfully exploit the continuum vulnerability.
7. I obtained a shell and fast environment of the machine.



# Evolution of Player 12's knowledge

| | |
|---|---|
| Etape 0 | P12 has an initial access on `n12-gateway`. |
| 1-<br>22ptblack<br>Etape 1 | P12 scanned network's services (T1046) from `n12-gateway` to `n12-vm1`. |
| Paramètres | $\mathbf{m} = \mathtt{n12-gateway}$, $\mathbf{u} = \mathtt{anonymous}$<br>$\mathbf{m}' = \mathtt{n12-vm1}$, $\Delta = \{\mathtt{top1000portsnmap}\}$ |
| Transition | $\mathcal{E}_1 = \mathcal{E}_0 \left[ \mathbf{m}' \leftarrow \left( \lfloor \mathbb{S}_{\mathbf{m}'} \rfloor_{\mathcal{E}_0} \cup \left\{ \begin{matrix} \mathsf{s}(\mathtt{port} : 8080), \\ \mathsf{s}(\mathtt{port} : 22), \\ \mathsf{s}(\mathtt{port} : 80), \\ \mathsf{s}(\mathtt{port} : 6697), \\ \mathsf{s}(\mathtt{port} : 3500) \end{matrix} \right\}, \lfloor \mathbb{P}_{\mathbf{m}'} \rfloor_{\mathcal{E}_0}, \lfloor \mathbb{A}_{\mathbf{m}'} \rfloor_{\mathcal{E}_0}, \lfloor \mathbb{N}_{\mathbf{m}'} \rfloor_{\mathcal{E}_0} \right) \right]$ |
| Trace<br>(net) | `21887 2021-05-09 20:07:49,695678 172.16.128.112 10.12.1.1`<br>`TCP 60 42548 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1357` |
| 1-<br>22ptblack<br>Etape 2 | P12 exploits a remote service (T1210) Apache Continuum (port 8080) from `n12-gateway` to `n12-vm1`. |
| Paramètres | $\mathbf{m} = \mathtt{n12-gateway}$, $\mathbf{u} = \mathtt{anonymous}$<br>$\mathbf{m}' = \mathtt{n12-vm1}$<br>$\mathsf{s} = \mathtt{continuum}(\mathtt{port} : 8080)$<br>$x = \text{EDB-ID} : 39945$ |
| Transition | $\mu_1 = \mu_0 \cup \{(\mathtt{n12-vm1}, \mathtt{root})\}$ |
| Trace<br>(net) | `170511 2021-05-09 20:28:15,698503 172.16.128.112 10.12.1.1`<br>`HTTP 1411 POST /continuum/saveInstallation.action HTTP/1.1` |
| 1-<br>22ptblack<br>Etape 3 | P12 a récupéré un premier fichier *flag* secret (T1083) sur $\mathtt{n12-vm1}$. |
| Paramètres | $\mathbf{m} = \mathtt{n12-vm1}$, $\mathbf{u} = \mathtt{root}$<br>$\mathsf{p} = \mathtt{/opt/apache\_continuum/apache-continuum-1.4.2/flag.txt}$ |
| Transition | $\mathcal{S}_1 = \mathcal{S}_0 \cup \{\mathtt{TvYSrSr6FwmMeXRVcUz6lkFQPZLBL2oj}\}$<br>$\mathcal{E}_2 = \mathcal{E}_1[\mathbf{m} \leftarrow (\lfloor \mathbb{S}_{\mathbf{m}} \rfloor_{\mathcal{E}_1}, \lfloor \mathbb{P}_{\mathbf{m}} \rfloor_{\mathcal{E}_1} \oplus \{(\mathsf{p}, \{\mathtt{root}\})\}, \lfloor \mathbb{A}_{\mathbf{m}} \rfloor_{\mathcal{E}_1}, \lfloor \mathbb{N}_{\mathbf{m}} \rfloor_{\mathcal{E}_1})]$ |
| Trace<br>(sys) | `May 9 20:28:54 n12-vm1 snoopy[1566]:`<br>`[uid:0 sid:1309 tty:(none) cwd:/opt/apache_continuum/apache-continuum-1.4.2/ filename:/bin/cat]: cat flag.txt` |

$$\{(\mathtt{n12-gateway}, \mathtt{anonymous})\}, \emptyset, \emptyset)$$

$$\downarrow \mathbf{t}_{1046}$$

$$(\{(\mathtt{n12-gateway}, \mathtt{anonymous})\ \}, \emptyset, \mathtt{n12-vm1} \leftarrow \left( \left\{ \begin{matrix} \mathsf{s}(\mathtt{port} : 8080), \\ \mathsf{s}(\mathtt{port} : 22), \\ \mathsf{s}(\mathtt{port} : 80), \\ \mathsf{s}(\mathtt{port} : 6697), \\ \mathsf{s}(\mathtt{port} : 3500) \end{matrix} \right\}, -, -, - \right) )$$

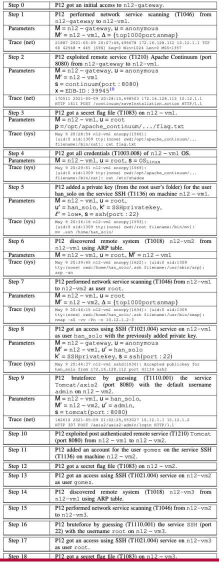
$$\downarrow \mathbf{t}_{1210}$$

$$(\{(\mathtt{n12-gateway}, \mathtt{anonymous}), (\mathtt{n12-vm1}, \mathtt{root})\}, \emptyset, \mathtt{n12-vm1} \leftarrow \left( \left\{ \begin{matrix} \mathsf{s}(\mathtt{port} : 8080), \\ \mathsf{s}(\mathtt{port} : 22), \\ \mathsf{s}(\mathtt{port} : 80), \\ \mathsf{s}(\mathtt{port} : 6697), \\ \mathsf{s}(\mathtt{port} : 3500) \end{matrix} \right. , -, -, - \right\} \Bigg)$$

$$\downarrow \mathbf{t}_{1083}$$

$$(\{(\mathtt{n12-gateway}, \mathtt{anonymous})\ \}, \mathtt{TvYSrSr6FwmMeXRVcUz6lkFQPZLBL2oj}, \mathtt{n12-vm1} \leftarrow \left( \left\{ \begin{matrix} \mathsf{s}(\mathtt{port} : 8080), \\ \mathsf{s}(\mathtt{port} : 22), \\ \mathsf{s}(\mathtt{port} : 80), \\ \mathsf{s}(\mathtt{port} : 6697), \\ \mathsf{s}(\mathtt{port} : 3500) \end{matrix} \right\}, \{\ (\mathtt{/opt/\ldots/flag.tx} \right.$$

# The complete attack campaign of Player 12

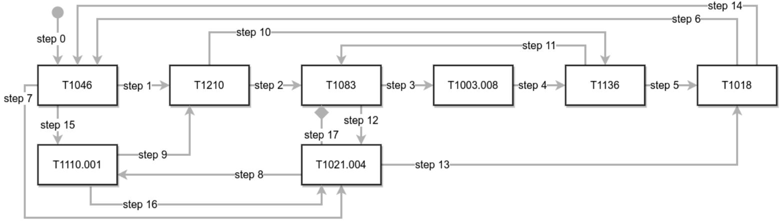


| | |
|---|---|
| Step 0 | P12 got an initial access to n12-gateway. |
| Step 1 | P12 performed network service scanning (T1046) from n12-gateway to n12-vm1. |
| Parameters | M = n12 − gateway, u = anonymous<br>M′ = n12 − vm1, Δ = {top1000portsnmap} |
| Trace (net) | 21887 2021-05-09 20:07:49,695678 172.16.128.112 10.12.1.1 TCP 60 42548 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1357 |
| Step 2 | P12 exploited remote service (T1210) Apache Continuum (port 8080) from n12-gateway to n12-vm1. |
| Parameters | M = n12 − gateway, u = anonymous<br>M′ = n12 − vm1<br>s = continuum(port : 8080)<br>x = EDB-ID : 39945[10] |
| Trace (net) | 170511 2021-05-09 20:28:15,698503 172.16.128.112 10.12.1.1 HTTP 1411 POST /continuum/saveInstallation.action HTTP/1.1 |
| Step 3 | P12 got a secret flag file (T1083) on n12 − vm1. |
| Parameters | M = n12 − vm1, u = root<br>p =/opt/apache_continuum/.../flag.txt |
| Trace (sys) | May 9 20:28:54 n12-vm1 snoopy[1566]: [uid:0 sid:1309 tty:(none) cwd:/opt/apache_continuum/... filename:/bin/cat]: cat flag.txt |
| Step 4 | P12 got all credentials (T1003.008) of n12 − vm1 OS. |
| Parameters | M = n12 − vm1, u = root, s = $OS_{Linux}$ |
| Trace (sys) | May 9 20:29:51 n12-vm1 snoopy[1569]: [uid:0 sid:1309 tty:(none) cwd:/opt/apache_continuum/... filename:/bin/cat]: cat /etc/shadow |
| Step 5 | P12 added a private key (from the root user's folder) for the user han_solo on the service SSH (T1136) on machine n12 − vm1. |
| Parameters | M = n12 − vm1, u = root,<br>u′ = han_solo, k′ = SSHprivatekey,<br>ℓ′ = low∗, s = ssh(port : 22) |
| Trace (sys) | May 9 20:36:16 n12-vm1 snoopy[1593]: [uid:0 sid:1309 tty:(none) cwd:/root filename:/bin/mv]: mv .ssh /home/han_solo/ |
| Step 6 | P12 discovered remote system (T1018) n12-vm2 from n12-vm1 using ARP table. |
| Parameters | M = n12 − vm1, u = root, M′ = n12 − vm1 |
| Trace (sys) | May 9 20:39:45 n12-vm1 snoopy[1622]: [uid:0 sid:1309 tty:(none) cwd:/home/han_solo/.ssh filename:/usr/sbin/arp]: arp -an |
| Step 7 | P12 performed network service scanning (T1046) from n12-vm1 to n12-vm2 as user root. |
| Parameters | M = n12 − vm1, u = root<br>M′ = n12 − vm2, Δ = {top1000portsnmap} |
| Trace (sys) | May 9 20:44:15 n12-vm1 snoopy[1634]: [uid:0 sid:1309 tty:(none) cwd:/home/han_solo/.ssh filename:/usr/bin/nmap]: nmap -sS -vv -Pn -n 10.12.1.2-3 |
| Step 8 | P12 got an access using SSH (T1021.004) service on n12-vm1 as user han_solo with the previously added private key. |
| Parameters | M = n12 − gateway, u = anonymous<br>M′ = n12 − vm1, u′ = han_solo<br>k′ = SSHprivatekey, s = ssh(port : 22) |
| Trace (sys) | May 9 20:44:37 n12-vm1 sshd[1636]: Accepted publickey for han_solo from 172.16.128.112 port 41134 ssh2 |
| Step 9 | P12 bruteforce by guessing (T1110.001) the service Tomcat/axis2 (port 8080) with the default username admin on n12 − vm2. |
| Parameters | M = n12 − vm1, u = han_solo,<br>M′ = n12 − vm2, u′ = admin,<br>s = tomcat(port : 8080) |
| Trace (net) | 182610 2021-05-09 21:02:25,553027 10.12.1.1 10.12.1.2 HTTP 307 POST /axis2/axis2-admin/login HTTP/1.1 |
| Step 10 | P12 exploited post authenticated remote service (T1210) Tomcat (port 8080) from n12 − vm1 to n12 − vm2. |
| Step 11 | P12 added an account for the user gomez on the service SSH (T1136) on machine n12 − vm2. |
| Step 12 | P12 got a secret flag file (T1083) on n12 − vm2. |
| Step 13 | P12 got an access using SSH (T1021.004) service on n12-vm2 as user gomez. |
| Step 14 | P12 discovered remote system (T1018) n12-vm3 from n12-vm1 using ARP table. |
| Step 15 | P12 performed network service scanning (T1046) from n12-vm2 to n12-vm3. |
| Step 16 | P12 bruteforce by guessing (T1110.001) the service SSH (port 22) with the username root on n12 − vm3. |
| Step 17 | P12 got an access using SSH (T1021.004) service on n12-vm3 as user root. |
| Step 18 | P12 got a secret flag file (T1083) on n12 − vm3. |

- 18 steps
- 6 attack techniques used
- 6 attack positions

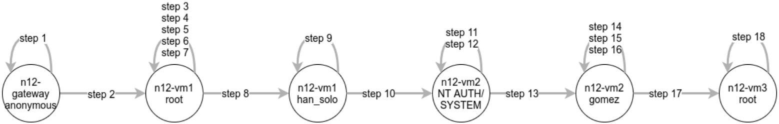
# First immediate benefit

You can visualize the attack from the attack techniques point of view



# First immediate benefits

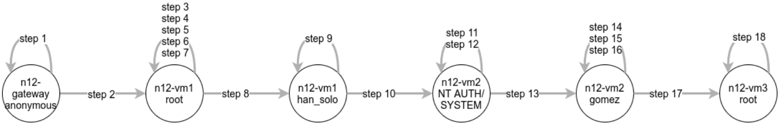
## You can visualize the propagation area



# Perspectives

## Attack scenario

- An attack position is a pair (*machine*, *user*)
- A successful attack procedure execution
  - increase the attacker knowledge
  - or allows to move from an attack position to another



# Take away

- PWNJUTSU : a new dataset of traces of professional attackers
- a semantic of attack techniques that allows to precisely describe the attacker behavior
- the central concept of attack position

# What is still missing ?

## In this work

- the dataset misses from noise and normal activity
- the logs were manually interpreted

## More globally

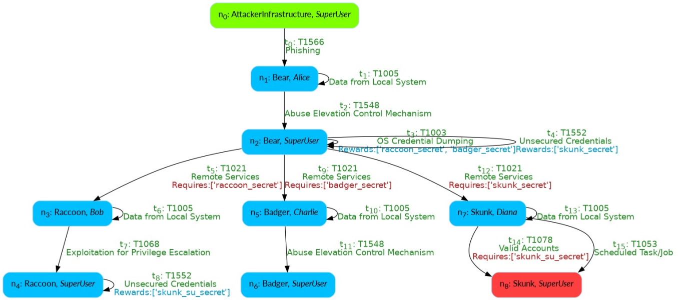
We need

- more precisely described datasets with different infrastructures and different attacks
- high level and low level representation of attacks
- a way to infer these representation automatically

# Perspectives

Submitted for publication. PhD thesis research project of Pierre-Victor Besson

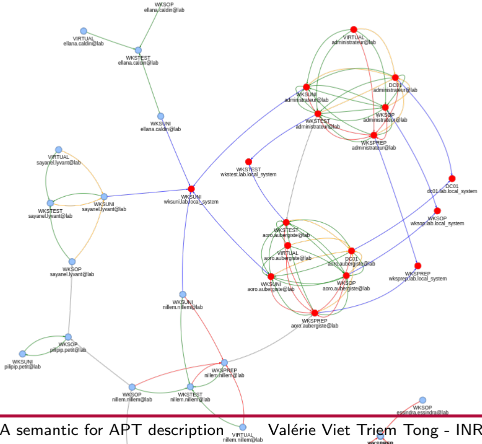
## Generation of training systems



## Perspectives

submitted for publication, to be improved during the PhD thesis research project of Manuel Poisson in collaboration with Amossys.

### Evaluation of the propagation area using Living-off-the-land techniques



WKSOP ellana.caldin@lab
VIRTUAL ellana.caldin@lab
WKSTEST ellana.caldin@lab
WKSUNI ellana.caldin@lab
VIRTUAL administrateur@lab
DC01 administrateur@lab
WKSUNI administrateur@lab
WKSOP administrateur@lab
WKSTEST administrateur@lab
WKSPREP administrateur@lab
WKSTEST wkstest.lab.local_system
VIRTUAL sayanel.lyvant@lab
DC01 dc01.lab.local_system
WKSUNI wksuni.lab.local_system
WKSUNI sayanel.lyvant@lab
WKSTEST sayanel.lyvant@lab
WKSOP wksop.lab.local_system
WKSTEST aoro.aubergiste@lab
VIRTUAL aoro.aubergiste@lab
DC01 aoro.aubergiste@lab
WKSOP sayanel.lyvant@lab
WKSPREP wksprep.lab.local_system
WKSUNI aoro.aubergiste@lab
WKSOP aoro.aubergiste@lab
WKSUNI nillem.nillem@lab
WKSPREP aoro.aubergiste@lab
WKSOP pilipip.petit@lab
WKSUNI pilipip.petit@lab
WKSPREP nillem.nillem@lab
WKSOP nillem.nillem@lab
WKSTEST nillem.nillem@lab
WKSOP essindra.essindra@lab
VIRTUAL nillem.nillem@lab
WKSPREP

# References I

Branka Stojanović, Katharina Hofer-Schmitz, and Ulrike Kleb.
Apt datasets and attack modeling for automated detection methods : A review.
*Comput. Secur.*, 92, 2020.

Catherine Beazley, Karan Gadiya, Ravi K U Rakesh, David Roden, Boda Ye, Brendan Abraham, Donald E. Brown, and Malathi Veeraraghavan.
Exploratory data analysis of a unified host and network dataset.
In *2019 Systems and Information Engineering Design Symposium (SIEDS)*, pages 1–5, 2019.

Sowmya Myneni, Ankur Chowdhary, Abdulhakim Sabur, Sailik Sengupta, Garima Agrawal, Dijiang Huang, and Myong Kang.
Dapt 2020 - constructing a benchmark dataset for advanced persistent threats.
In *Deployable Machine Learning for Security Defense - 1st International Workshop, MLHat 2020, Proceedings*, Communications in Computer and Information Science. Springer Science and Business Media Deutschland GmbH, 2020.

Aimad Berady, Mathieu Jaume, Valérie Viet Triem Tong, and Gilles Guette.
PWNJUTSU : A dataset and a semantics-driven approach to retrace attack campaigns.
*IEEE Transactions on Network and Service Management*, 2022.

# References II

Aimad Berady, Valérie Viet Triem Tong, Gilles Guette, Christophe Bidan, and Guillaume Carat.
Modeling the Operational Phases of APT Campaigns.
In *CSCI 2019 - 6th Annual Conf. on Computational Science & Computational Intelligence*, Las Vegas, United States, December 2019.