

Copy-and-Paste-APT

Ein Pentesters' Guide zur Threat Emulation

Darius Beckert & Nicolas Aversch

XSEC infosec GmbH
Mayerhofgasse 6
1040 Vienna

07.10.2022



Introduction: Who are we?

Darius B.

- IT-Security Consultant
- APTs, Malware Analysis, Capture-The-Flag Events
- OSCP, ISO 27001 Foundation

Nicolas A.

- IT-Security Consultant
- APTs, Mathematik, OpenBSD

Threat Emulation vs. Pentest

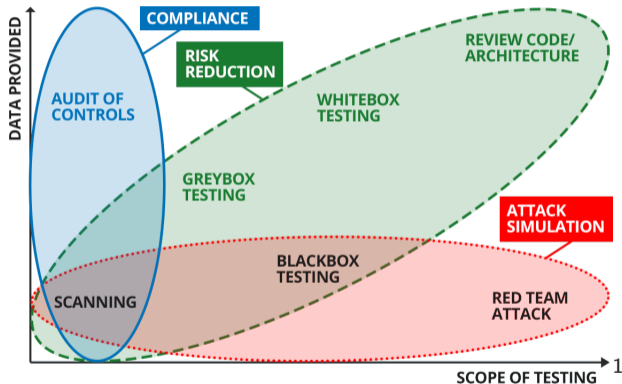
Klassischer Pentest

- Zeitrahmen: 1-2 Wochen
- Weite Abdeckung
- Flach (1 bis 2 Systeme, wenige Webseiten, etc.)

Threat Emulation

- Zeitrahmen: 1-4 Wochen
- Schmale Abdeckung
- Tief (Phishing, Firewall, internes Netzwerk, etc)

Threat Emulation vs. Pentest



¹<https://www.infosecpartners.com/cyber-security-testing-and-compliance/penetration-testing-services-pentest>

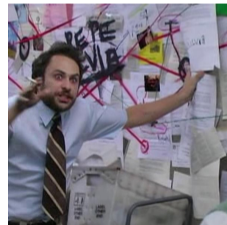
Wieso nicht beides?

- Zeitrahmen: 1 Woche
 - 1 Angriffsphase/Tag
 - Konstante Kommunikation mit Auftraggeber/Blue Team
 - Informationen werden vom Auftraggeber während der Prüfung zur Verfügung gestellt
 - Whitebox-Test mit Fokus auf Threat Actor “Tactics, Techniques and Procedures” (TTP)
 - Basierend auf Open-Source-Projekten & -Informationen
- ⇒ Verringerter Ressourcen-Aufwand für Pentester und Auftraggeber

Einleitung in die MITRE ATT&CK Matrix



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Account Discovery	Account Hijacking	Account Manipulation	Application Hijacking	Application Persistence	Application Spoofing	Application Whitelisting	Application Whitelisting	Application Whitelisting	Application Whitelisting	Application Whitelisting	Application Whitelisting	Application Whitelisting	Application Whitelisting
...



2

Einleitung in die MITRE ATT&CK Matrix

Tactics

- Initial Access
- Privilege Escalation
- Defense Evasion
- Lateral Movement
- ...

Techniques sind Taktiken zugeordnet

- Technique: Phishing (T1566)
- Tactic: Initial Access (TA0001)

Einleitung in die MITRE ATT&CK Matrix

- Threat Actor Liste mit zugeordneten TTPs (inklusive Quellen)



The screenshot shows a web browser window with the URL <https://attack.mitre.org/groups/>. The page features a red navigation bar with the MITRE ATT&CK logo and links for Matrices, Tactics, Techniques, Blog, and Contribute. A search bar is also present. Below the navigation bar, a blue banner announces the new v11.2 release of MITRE ATT&CK, which includes a beta version of Sub-Techniques. The main content area is titled "Groups" and includes a breadcrumb "Home > Groups". The text explains that Groups are sets of related intrusion clusters of activities using various intrusion sets, and campaigns. It also mentions that some organizations track similar activities designated by other organizations. A sidebar on the left lists "GROUPS" with an "Overview" link and a list of threat actors: admin@338, Ajax Security Team, ALLANITE, Andariel, and APT-C-36.

³<https://attack.mitre.org/groups/>

Einleitung in die MITRE ATT&CK Matrix

The screenshot shows the MITRE ATT&CK website interface. The top navigation bar includes links for Matrices, Tactics, Techniques, Data Sources, Mitigations, Groups, Software, and Resources. The main content area is titled "GOLD SOUTHFIELD" and provides a description of the group, its ID (G0115), contributors, version, and creation/modification dates. Below this, a section titled "Techniques Used" contains a table with two entries.

GROUPS

- GOLD SOUTHFIELD
- Gorgon Group
- Group5
- HAFNIUM
- HEXANE
- Higaisa
- Honeybee
- Inception
- IndigoZebra
- Indrik Spider
- Ke3chang
- Kimsuky
- Lazarus Group
- LazyScripter

GOLD SOUTHFIELD

GOLD SOUTHFIELD is a financially motivated threat group active since at least 2019 that operates the REvil Ransomware-as-a Service (RaaS). GOLD SOUTHFIELD provides backend infrastructure for affiliates recruited on underground forums to perpetrate high value deployments.^{[1][2][3]}

ID: G0115
Contributors: Thijn Bukkems, Amazon
Version: 1.1
Created: 22 September 2020
Last Modified: 26 April 2021

Version Permalink

ATT&CK® Navigator Layers

Techniques Used

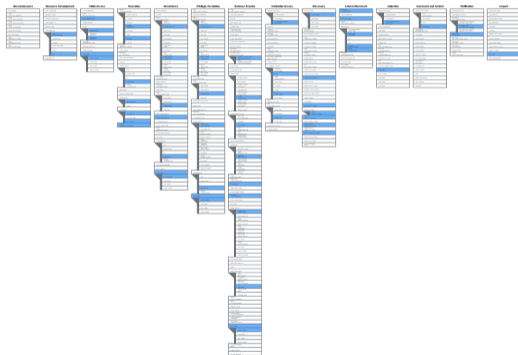
Domain	ID	Name	Use
Enterprise	T1059	Command and Scripting Interpreter: PowerShell	GOLD SOUTHFIELD has staged and executed PowerShell scripts on compromised hosts. ^[4]
Enterprise	T1190	Exploit Public-Facing Application	GOLD SOUTHFIELD has exploited Oracle WebLogic vulnerabilities for initial compromise. ^[1]

4

⁴<https://attack.mitre.org/groups/G0115>

Einleitung in die MITRE ATT&CK Matrix

Gruppe: Wizard Spider (G0102) (TrickBot, Ryuk)⁵



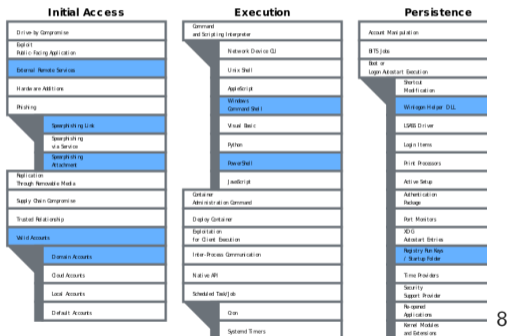
6

⁵<https://attack.mitre.org/groups/G0102/>

⁶<https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0102%2FG0102-enterprise-layer.json>

Angriffsplanung mit der ATT&CK Matrix

Gruppe: Wizard Spider (G0102) (TrickBot, Ryuk)⁷



8

⁷<https://attack.mitre.org/groups/G0102/>

⁸<https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0102%2FG0102-enterprise-layer.json>

Vorbereitungsphase: Kunde

Klare Kommunikationswege (Team, Auftraggeber/Blue Team)

- Backup parat haben! (z.B. Telefonnummer, E-Mail, etc.)
- Kommunikationskanäle **vor** der Prüfung testen!

Scoping!

- Was will das Blue Team mit dem Test erreichen?
- Wo liegt kritische Infrastruktur?
- Besonderes Augenmerk?
- Was ist erlaubt/sind die Risiken bekannt?

(Ideal) Zugriff mit "normalem" Benutzer auf eine Workstation

Vorbereitungsphase: Infrastruktur

Keine Zeit für Hot-Patching!



Vorbereitungsphase: Infrastruktur

- Sehr kurzer Test + Ankündigung beim Blue Team = Verschleierung entfällt (zum Teil!)
- 1 Domain-Name
 - Ideal: unscheinbare und kurze Namen (file-host.com, docscloud.at, etc.)
- 1 Command & Control (C2) Server
- Reproduzierbare Infrastruktur (Ansible, Docker!)

Vorbereitungsphase: Infrastruktur

Ansible:

- IT Automation
- „Infrastructure as code“

```
1 ---
2 ▼ - name: Update web servers
3   hosts: webservers
4   remote_user: root
5
6   tasks:
7 ▼ - name: Ensure apache is at the latest version
8 ▼   ansible.builtin.yum:
9     name: httpd
10    state: latest
11 ▼ - name: Write the apache config file
12 ▼   ansible.builtin.template:
13     src: /srv/httpd.j2
14     dest: /etc/httpd.conf
15
16 ▼ - name: Update db servers
17   hosts: databases
18   remote_user: root
19
20   tasks:
21 ▼ - name: Ensure postgresql is at the latest version
22 ▼   ansible.builtin.yum:
23     name: postgresql
24     state: latest
25 ▼ - name: Ensure that postgresql is started
26 ▼   ansible.builtin.service:
27     name: postgresql
28     state: started
```

Vorbereitungsphase: Infrastruktur

Docker:

- OS-level Virtualisierung
- Software-Paket – Container
- Reproduzierbare Infrastruktur

```
1 FROM debian:bullseye
2
3 LABEL maintainer="@cyb3rn0dl3s <https://github.com/cyb3rn0dl3s>"
4
5 ENV DEBIAN_FRONTEND=noninteractive DEBCONF_NONINTERACTIVE_SEEN=true
6
7 # Create sliver user & group
8 RUN useradd --uid 10000 -m -s /usr/sbin/nologin -U sliver
9
10 # Update & install required packages
11 RUN apt update && apt install --no-install-recommends -y curl ca-certificates
12 mingw-w64 binutils-mingw-w64 g++-mingw-w64 && rm -rf /var/lib/apt/lists/*
13
14 # Metasploit (optional) dependency -- this will make the container CI
15 RUN mkdir /opt/install
16 WORKDIR /opt/install/
17 RUN curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/
18 framework-wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall
19 rf install
20
21 # Install sliver
22 USER sliver
23 WORKDIR /home/sliver
```


Vorbereitungsphase: Infrastruktur

- „Einkaufsliste“
 - Command & Control
 - Metasploit Framework (metasploitframework/metasploit-framework:latest) ⁹
 - Empire (S0363) (bcsecurity/empire:latest) ¹⁰
 - Sliver (S0633) (ghcr.io/cyb3rn00dl3s/container-sliver:latest)¹¹
 - Obfusieren & Verschlüsseln
 - PEzor ¹²
 - Veil-Evasion ¹³
 - Web Server für Delivery und Exfiltration
 - Nginx (nginx:alpine)

⁹<https://github.com/rapid7/metasploit-framework>

¹⁰<https://github.com/BC-SECURITY/Empire>

¹¹<https://github.com/cyb3rn00dl3s/container-sliver>

¹²<https://github.com/Nahid5/pezor-docker>

¹³<https://github.com/Veil-Framework/Veil>

Vorbereitungsphase: Infrastruktur

Ansible + Docker + tmuxify¹⁴ = Automatische Infrastruktur in Sekunden!

```
> time ansible-playbook roles/debian/full_install.yml
[WARNING]: An error occurred while calling ansible.utils.display.initialize_locale
(unsupported locale setting). This may result in incorrectly calculated text widths that
can cause Display to print incorrect line lengths

PLAY [Full Debian install] *****

TASK [Gathering Facts] *****
ok: [c2Host ]

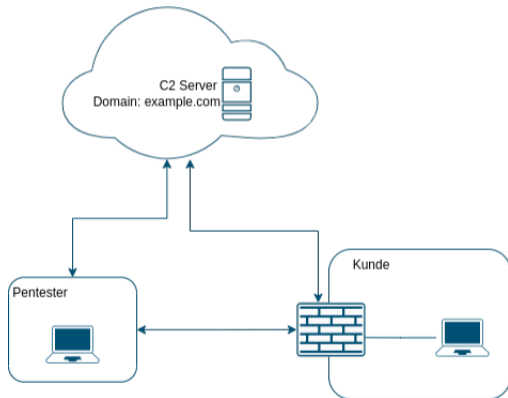
PLAY RECAP *****
{{ c2Host }} : ok=46  changed=27  unreachable=0  failed=0  skipped=0
rescued=0  ignored=0

ansible-playbook roles/debian/full_install.yml 37.22s user 6.80s system 14% cpu 5:05.29 to
tal
```

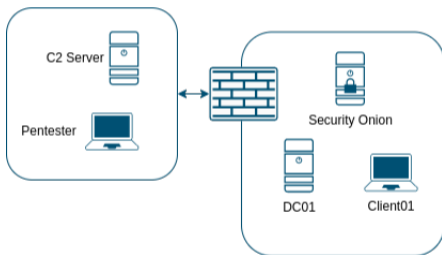
305 Sekunden!

¹⁴<https://github.com/tonchis/tmuxify>

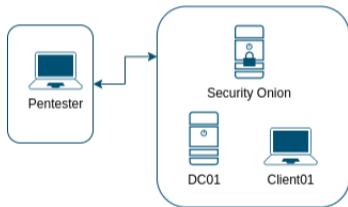
Vorbereitungsphase: Infrastruktur



Vorbereitungsphase: Infrastruktur (Labor)



Vorbereitungsphase: Infrastruktur (Labor)



Vorbereitungsphase: Infrastruktur (Labor)

mytext

Vorbereitungsphase: AV Evasion

- Verteidigung sichten (Absprache mit Auftraggeber!)
- Eigenen Loader schreiben → Alles weitere den C2 machen lassen!
- Punkte der möglichen Erkennung beachten!
 - Netzwerk (NIDS/-IPS)
 - HTTPS - gut aber schützt nicht vor DPI!
 - Client (AV/EDR/EDX)
 - Ausführen von Powershell und C Programmen (AMSI ETW)
 - Verhalten von Programmen (*-Injection, API Calls, etc.)
 - Dateien lesen & schreiben
 - Applikationsebene (Mail Transfer Agent (MTA))

Vorbereitungsphase: AV Evasion

Rule of Thumb

- Alles verschlüsseln
- In (fremdem) Speicher arbeiten
- „Living Off The Land“ – Mit vorhandenen Tools der Umgebung arbeiten
 - <https://lolbas-project.github.io/>

⇒ Mitre ATTACK: Quellen beinhalten Verhalten von Threat Actor!

Initial Access

- Erfolgreiches Phishing simulieren
 - „Benutzer, der fast alles klickt“
- E-Mail als gefährlichstes Einfallstor
- Links / Applikationen im Internet an zweiter Stelle

Initial Access

- Excel Macros immer häufiger von MTAs erkannt
 - Starke Obfuskierung → Makros sind sprachabhängig
- Siehe z.B. EXCELntDonut¹⁵
- Eigene Obfuskierung und Verschlüsselung ad-hoc schreiben: Zeitaufwändig!

¹⁵<https://github.com/FortyNorthSecurity/EXCELntDonut>

Initial Access

- Lösung:
 - Word Makros
 - docx, docm, docb... Falls ein Format hängen bleibt, ein anderes Format nehmen
 - Selbst nicht-obfuskiert nur als "Risiko" am MTA eingestuft
 - Bemühungen seitens Microsoft diese standardmäßig zu deaktivieren
 - Office-URI ¹⁶
 - `ms-excel:ofv|u|https://contoso/Q4/budget.xls`
 - umgeht Mail-Filter aber nicht Firewall!
 - Keine Makros: LNK-Datei + ISO-Datei ¹⁷

¹⁶<https://docs.microsoft.com/en-us/office/client-developer/office-uri-schemes>

¹⁷<https://v3ded.github.io/redteam/abusing-lnk-features-for-initial-access-and-persistence>

Initial Access

- Detektierung und Verhinderung
 - Makro-Angriffe
 - Word, Excel und Powerpoint Dateiformate mit Makros filtern
 - Office-URI
 - Office-URI am MTA in der E-Mail erkennen
 - Firewall mit Anti-Viren-Scan/Makro Erkennung
 - LNK-Datei + ISO-Datei
 - Sollten aus E-Mails und Web-Traffic gefiltert werden

C2 Kommunikation

- Unauffälliger Domain Name
 - Nicht erst kurz vor der Prüfung registrieren!
- HTTPS (T1071.001)
 - Eigene Zertifikate erstellen
 - Müssen nicht valide sein
 - Tauchen somit auch nicht im CT Record auf!
 - DPI umgeht Verschlüsselung
 - Traffic wie unverschlüsselt behandeln
 - Trotzdem verschlüsseln!
- Keine zufälligen Ports (HTTPS auf 443, HTTP auf 80, etc)!

C2 Kommunikation

HTTP als Tarnung (malleable C2) (T1001.003)

```

#
# Amazon browsing traffic profile
#
# Author: @harmj0y

set sleeptime "5000";
set jitter "0";
set maxdns "255";
set useragent "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko";

http-get {
  set uri "/s/ref-nb_sb_noss_1/167-3294888-0262949/field-keywords=books";
  client {
    header "Accent" "**/*";
    header "Host" "www.amazon.com";
    metadata {
      base64;
      prepend "session-token=";
      prepend "skin=noskin;";
      append "csm-hit-s-24KU11B882RZSYGJ380K|1419899012996";
      header "Cookie";
    }
  }
  server {
    header "Server" "Server";
    header "x-amz-id-1" "THKUYEZKCKPGYST42PZT";
    header "x-amz-id-2" "a21yZ2xrND0tdGRsa212bGV3YW85amZuZW9ydG5rZnRuZ2tnZGl4aHRvNDVpbG0=";
    header "X-Frame-Options" "SAMEORIGIN";
    header "Content-Encoding" "gzip";
  }
  output {
    print;
  }
}

```

18

C2 Kommunikation

```
report-uri https://metrics.media-amazon.com/  
content-type: text/html;charset=UTF-8  
date: Thu, 30 Jun 2022 07:34:35 GMT  
expires: -1  
permissions-policy: interest-cohort=()  
pragma: no-cache  
server: Server  
set-cookie: session-token="LN7v5hpFx608qdPmW82Gqa/Wkrl8iP4p73WzVV2CrJ9hUhptL8QirKUG6uexzzqwg7VaZBbh7hdquo295IcFfC  
F+DwvlHWEVraUtIMUL1958RvYFrW+96Rh28oC6perFwJJXWQpMvZRTcc/I+UamPSosPtsVy59UZtCM+dWnSvZ1UQy72zi3FYirWvx0VANbILsYq5  
hHzAu65WRhN7M3w="; Version=1; Domain=.amazon.com; Max-Age=31536000; Expires=Fri, 30-Jun-2023 07:34:35 GMT; Path  
=/: Secure  
set-cookie: skin=noskin; path=/; domain=.amazon.com  
strict-transport-security: max-age=47474747; includeSubDomains; preload  
vary: Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent  
x-amz-rid: PXM4F3A6JRKJ2KJ0MCGE
```

⇒ Nicht auf Presets vertrauen!

C2 Kommunikation

- Empire hat nur limitierte Unterstützung für Malleable Profile
- Eigene Einstellungen für URL, Header, Cookies, UA, etc.

C2 Kommunikation

DefaultProfile <code>/admin/get.php,/news.php,/login/process.php Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0)</code>	Default communication profile for the agent.
Headers <code>Server:Microsoft-IIS/7.5</code>	Headers for the control server.
JA3_Evasion <code>False</code>	Randomly generate a JA3/S signature using TLS ciphers.
Launcher <code>powershell -noP -sta -w 1 -enc</code>	Launcher string.
StagingKey <code>aqvxd7HO{j78tAC@}FhrE3~4!&:R>U</code>	Staging key for initial agent negotiation.
Optional Fields	
CertPath	Certificate path for https listeners.
Cookie <code>beJihXKSG</code>	Custom Cookie Name

C2 Kommunikation

▼ Hypertext Transfer Protocol

```
> GET /news.php HTTP/1.1\r\n> Cookie: beJihXKSG=aF4DGuvozdImR7GFP31myYtEwwA=\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nHost: 10.1.2.5\r\nConnection: Keep-Alive\r\n\r\n\r\n[Full request URI: http://10.1.2.5/news.php]\n[HTTP request 1/1]\n[Response in frame: 6306]
```

C2 Kommunikation

- Kenne deine Tools
- **Teste** deine Tools

mytext

```
HTTP/1.1 200 OK · Server: Werkzeug/ 2.1.2 Python/3.9.13 · Date: Mon, 19 Sep 2022 13:24:45 GMT · Content-Type: text/html; charset=utf-8 · Content-Length: 7389 · Cache-Control: no-cache, no-store, must-revalidate · Pragma: no-cache · Expires: 0 · Server: Microsoft-IIS/ 7.5 · Connection: close · ·
```

C2 Kommunikation

Sehr interessant. Das kommt wohl vom ausgeführten Powershell Empire Agent.

C2 Kommunikation

Sehr interessant. Das kommt wohl vom ausgeführten Powershell Empire Agent.

Läuft er?

C2 Kommunikation

Sehr interessant. Das kommt wohl vom ausgeführten Powershell Empire Agent.

Läuft er?

Ja

C2 Kommunikation

Läuft er?

Gratuliere

Ja

Xsec

C2 Kommunikation

Gratuliere

Kann er nachhause telefonieren auch?

Ja

C2 Kommunikation

Gratuliere

Kann er nachhause telefonieren auch?

Ja, die Verbindung besteht immer noch

C2 Kommunikation

Kann er nachhause telefonieren auch?

Ja, die Verbindung besteht immer noch

Oh fuck 😊

C2 Kommunikation

Ja, die Verbindung besteht immer noch

Oh fuck 😊

(tschuldigung) 😊

C2 Kommunikation

mytext

Privilege Escalation

- Enumeration, Enumeration, Enumeration!
 - Schwachpunkte am Client und im Netzwerk finden.
 - Scripts/Befehle aus ATTACK nutzen!
 - Häufig bereits als Empire Modul integriert!

Privilege Escalation

- „Laute“ (OPSEC unsichere!) Tools beschleunigen die Phase
 - Winpeas (Windows Privilege Escalation Awesome Scripts) ¹⁹
 - Empire Modul: powershell/privesc/winpeas

⇒ Abhängig vom Scope/Ziel des Tests

¹⁹<https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS>

Privilege Escalation

- PrivEsc muss nicht unbedingt lokal sein!
- LDAP Queries absetzen
 - AdFind (S0552) ²⁰
- Den Hund im Wald spazieren lassen
 - Bloodhound (S0521) ²¹
 - Automatisches Enumerieren der Domäne

²⁰<http://www.joeware.net/freetools/tools/adfind/>

²¹<https://github.com/BloodHoundAD/BloodHound>

Privilege Escalation

DOMAIN COMPUTERS@CONTOSME.COM

Database Info Node Info Analysis

CONTOSME.COM

OVERVIEW

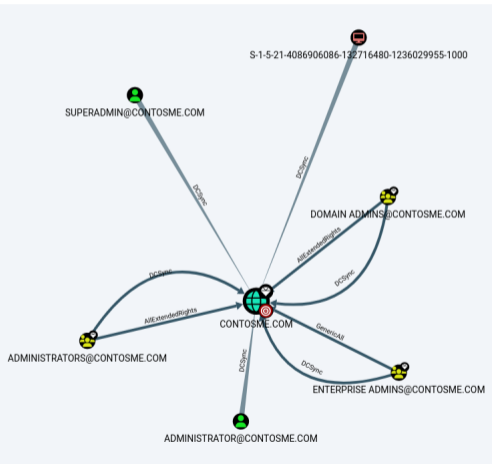
Users	6
Groups	52
Computers	0
OUs	6
GPOs	2
Map OU Structure	

NODE PROPERTIES

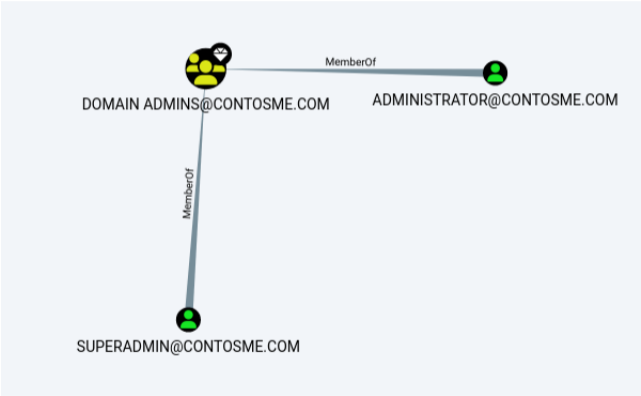
Object ID	S-1-5-21-4086906086-132716480-1236029955
Domain Functional Level	2016

EXTRA PROPERTIES

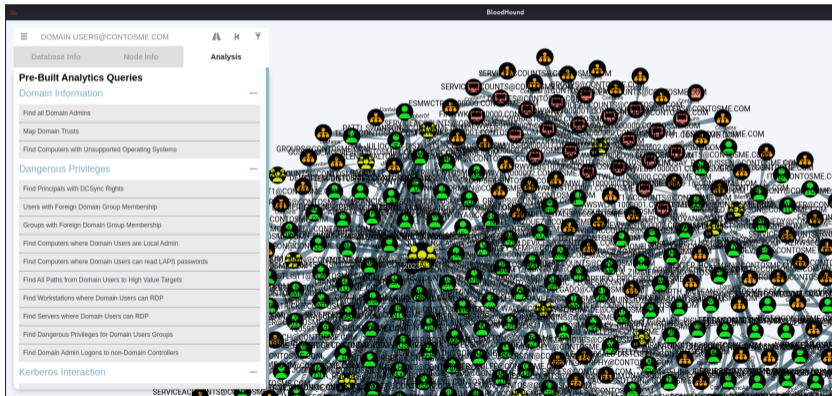
distinguishedname	DC=CONTOSME,DC=COM
domain	CONTOSME.COM
domainsid	S-1-5-21-4086906086-132716480-1236029955
whencreat	Wed, 27 Jul 2022 09:14:16 GMT



Privilege Escalation



Privilege Escalation



Privilege Escalation

mytext

Privilege Escalation

- Ergebnisse der Enumeration verwenden
- Authentifizierungen (NTLM/Kerberos)
- AD Fehlkonfigurationen
 - (Un-)Constrained Delegations
 - ACLs
 - ...

Lateral Movement

- Ausweitung im Netzwerk
 - Voraussetzung: Scope
- Netzwerkshare-Berechtigungen!
 - Endpoint Management/Software Deployment
 - Dokument-Shares mit Schreibrechten
 - Source Code
 - ...

Lateral Movement

- Nach Credential Access (TA0006) – Pivoting
- RDP (T1021.001), WinRM (T1021.006)
- Proxying von Tools (T1090)
 - Metasploits “autoroute” ²²
 - Sliver SOCKS5/Wireguard Reverse Proxy ²³

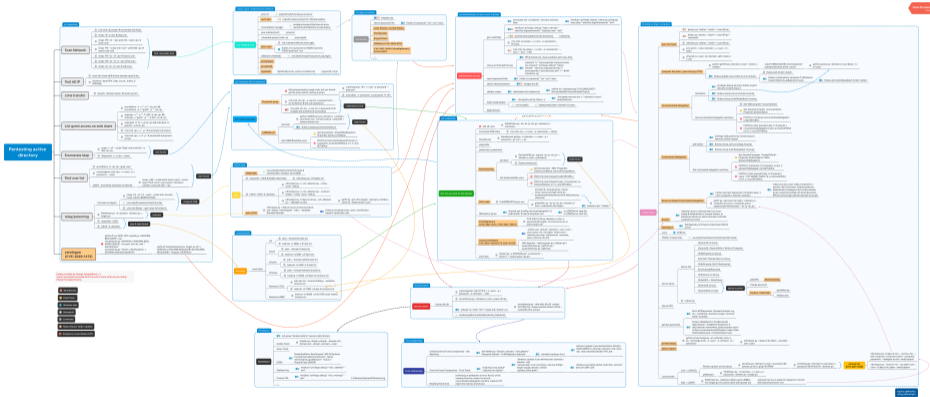
²²<https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/post/multi/manage/autoroute.md>

²³<https://github.com/BishopFox/sliver/wiki/Reverse-SOCKS>

Lateral Movement

- Patch-Level der Server beachten!
 - Regelmäßig Remote Command Execution (RCE) Schwachstellen!
 - RCE auf Domain-Controller = \$\$\$

Review



Takeaways

- Viele Open-Source Tools zur Verfügung
- Auf Datenbanken und deren Quellen zurückgreifen (MITRE ATT&CK)
 - Toolsets basierend auf Threat Actor zusammenstellen
- Wenig Eigenentwicklungen notwendig
 - Wissen über Funktionalitäten trotzdem wichtig!
- Wiederholbare Aufgaben automatisieren – Ressourcen sparen!
- Pentest ⇒ Keine komplette Killchain notwendig

Tool Zeit!

<https://github.com/cyb3rn00dl3s/container-sliver>

Public Pin Unwatch 1 Fork 0 Star 0

Code Issues Pull requests Discussions Actions Projects Wiki Security

latest Go to file Add file Code About

cyb3rn00dl3s added DNS port ... 22 days ago 5

.github/workflows	Adjusted branch and tag name, Readme ch...	28 days ago
Dockerfile	added DNS port	22 days ago
README.md	added DNS port	22 days ago
docker-compose.yml	added DNS port	22 days ago

README.md

Simple Sliver C2 Docker Container

docker dockerfile docker-image
sliver red-team security-tools
c2 red-team-engagement
command-and-control red-teaming

Readme
0 stars
1 watching
0 forks

Tool Zeit! (x2)

`https://github.com/cyb3rn00dl3s/attack-infrastructure`



(nur mit Erlaubnis)