Copy-and-Paste-APT

Ein Pentesters' Guide zur Threat Emulation

Darius Beckert & Nicolas Averesch

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

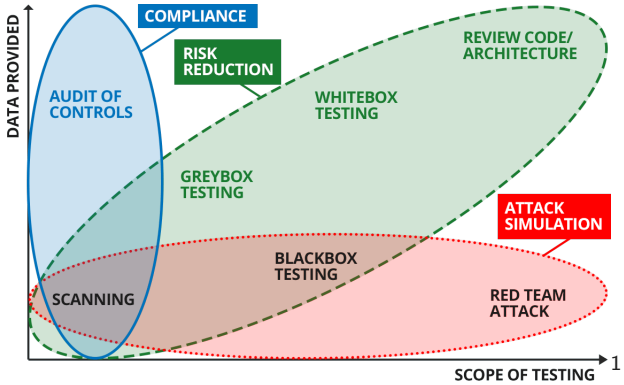
Klassischer Pentest

- 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



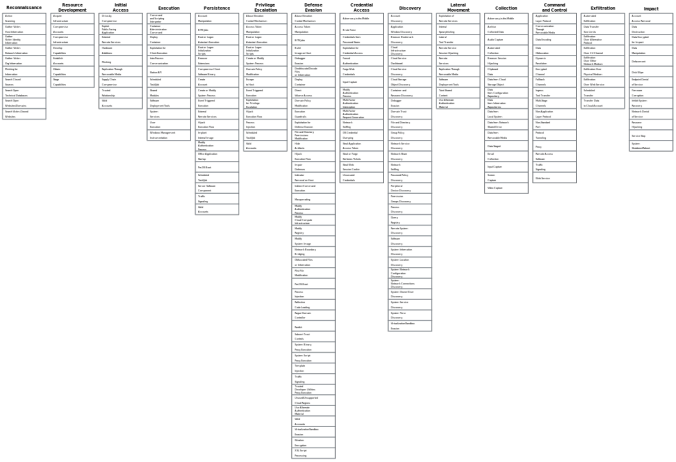
[1] https://www.infosecpartners.com/cyber-security-testing-and-compliance/penetration-testing-services-pentest

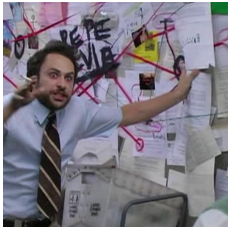
Wieso nicht beides?

- 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

$\Rightarrow$ Verringerter Ressourcen-Aufwand für Pentester und Auftraggeber

Einleitung in die MITRE ATT&CK Matrix





2

[2] https://attack.mitre.org/

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)

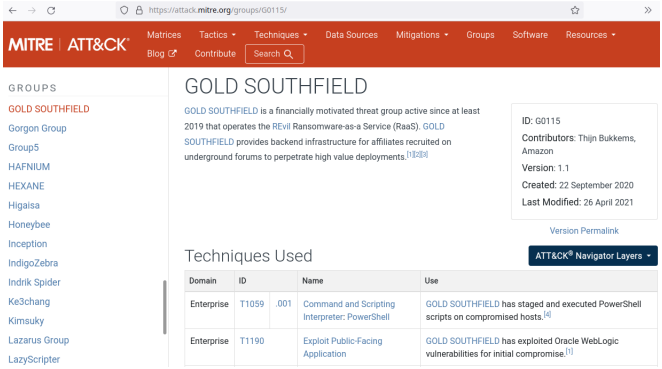
Einleitung in die MITRE ATT&CK Matrix

- Threat Actor Liste mit zugeordneten TTPs (inklusive Quellen)

[3]

[3] https://attack.mitre.org/groups/

Einleitung in die MITRE ATT&CK Matrix



4

[4] https://attack.mitre.org/groups/G0115

Einleitung in die MITRE ATT&CK Matrix

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

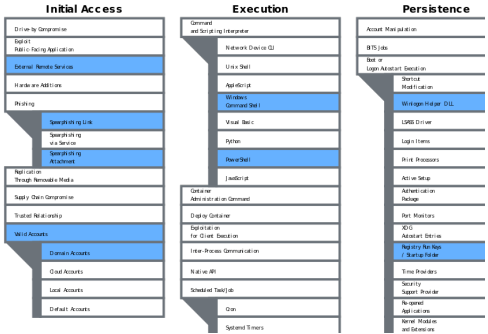
6

[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“

```yaml
---
- name: Update web servers
  hosts: webservers
  remote_user: root

  tasks:
  - name: Ensure apache is at the latest version
    ansible.builtin.yum:
      name: httpd
      state: latest
  - name: Write the apache config file
    ansible.builtin.template:
      src: /srv/httpd.j2
      dest: /etc/httpd.conf

- name: Update db servers
  hosts: databases
  remote_user: root

  tasks:
  - name: Ensure postgresql is at the latest version
    ansible.builtin.yum:
      name: postgresql
      state: latest
  - name: Ensure that postgresql is started
    ansible.builtin.service:
      name: postgresql
      state: started
```

Vorbereitungsphase: Infrastruktur

Docker:

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

```
FROM debian:bullseye

LABEL maintainer="@cyb3rn00dl3s <https://github.com/cyb3rn00dl3s>"

ENV DEBIAN_FRONTEND=noninteractive DEBCONF_NONINTERACTIVE_SEEN=true

# Create sliver user & group
RUN useradd --uid 10000 -m -s /usr/sbin/nologin -U sliver

# Update & install required packages
RUN apt update && apt install --no-install-recommends -y curl ca-cer
↪ mingw-w64 binutils-mingw-w64 g++-mingw-w64 && rm -rf /var/lib/apt/li

# Metasploit (optional) dependency -- this will make the container C
RUN mkdir /opt/install
WORKDIR /opt/install/
RUN curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus,
↪ framework-wrappers/msfupdate.erb > msfinstall && chmod 755 msfinsta
↪ rf install

# Install sliver
USER sliver
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]
  - Obfuskieren & 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

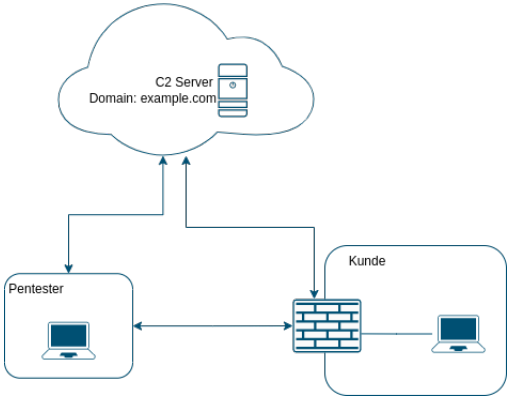
Ansible + Docker + tmuxify[14] = Automatische Infrastruktur in Sekunden!

```
❯ 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
```

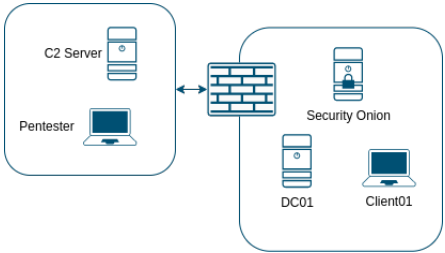
305 Sekunden!

[14] https://github.com/tonchis/tmuxify

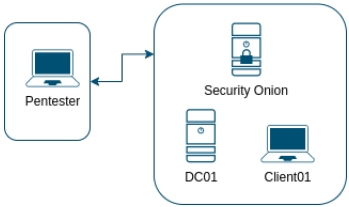
Vorbereitungsphase: Infrastruktur



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. EXCELntDonut[15]
- 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 (mallable 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 "Accept" "*/*";
        header "Host" "www.amazon.com";

        metadata {
            base64;
            prepend "session-token=";
            prepend "skin=noskin;";
            append "csm-hit=s-24KU11BB82RZSYGJ3BDK|1419899012996";
            header "Cookie";
        }
    }

    server {

        header "Server" "Server";
        header "x-amz-id-1" "THKUYEZKCKPGY5T42PZT";
        header "x-amz-id-2" "a21yZXxrNDNtdGRsa212bGV3YW85amZuZW9ydG5rZmRuZ2tmZGl4aHRvNDVpbgo=";
        header "X-Frame-Options" "SAMEORIGIN";
        header "Content-Encoding" "gzip";

        output {
            print;
        }
    }
}
```

18

[18] https://raw.githubusercontent.com/rsmudge/Malleable-C2-Profiles/master/normal/amazon.profile

C2 Kommunikation

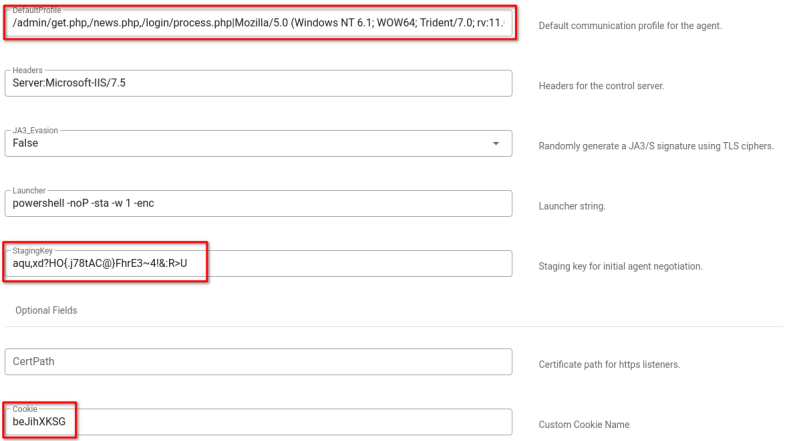
```
report-uri https://metrics.media-amazon.com/
content-type: text/html;charset=UTF-8
date: Thu, 30 Jun 2022 07:34:35 GMT
expires: -1
permissions-policy: interest-cohort=()
pragma: no-cache
server: Server
set-cookie: session-token="LN7v5hpFx608qdPmW82Gqa/Wkrl8iP4p73WzVV2CrJ9hUhptL8QirKUG6uexzzqwg7VaZBbh7hdquo295IcfFc
F+DuwlHWEVraUtIMUL1958RvYFrW+96Rh28oC6perFwJJXWQpMvZRTCc/I+UamPSosPtsVy59UZtCM+dWnSvZiUQy72zi3FYirWvx0VAnbIlsYq5
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!

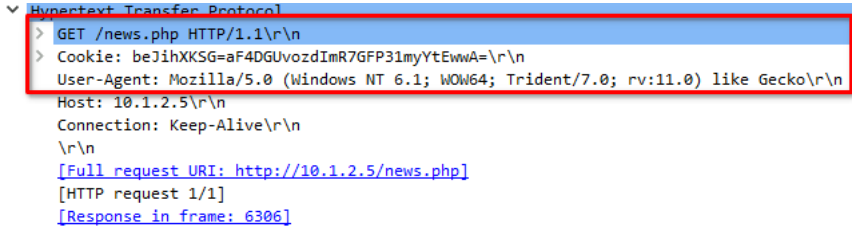
C2 Kommunikation

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

C2 Kommunikation



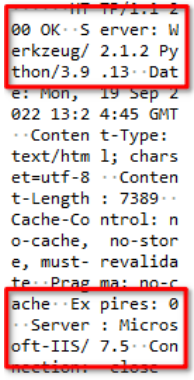
C2 Kommunikation



C2 Kommunikation

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

mytext



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?

Ja

Gratuliere

C2 Kommunikation

Ja

Gratuliere

Kann er nachhause telefonieren auch?

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

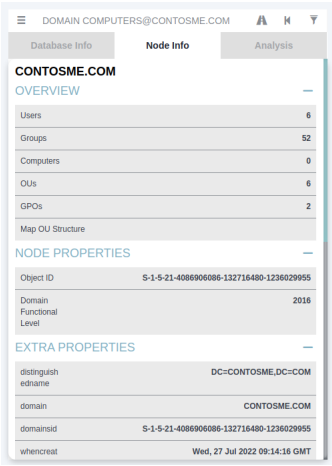
[19] https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

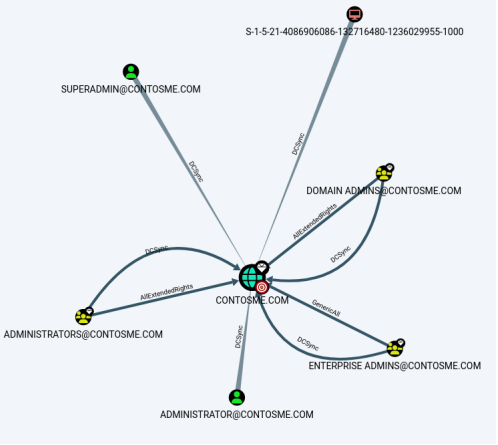
Privilege Escalation

- 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

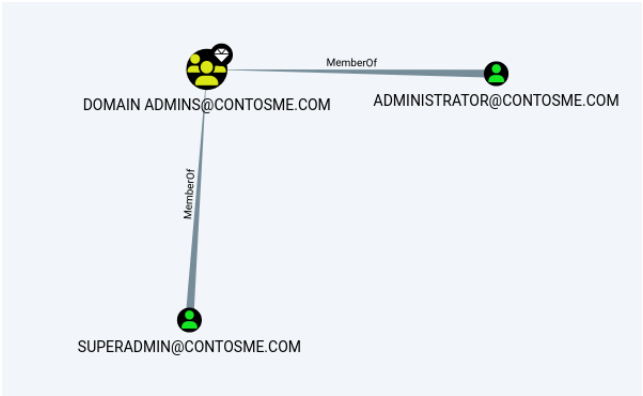
[20] http://www.joeware.net/freetools/tools/adfind/
[21] https://github.com/BloodHoundAD/BloodHound

Privilege Escalation

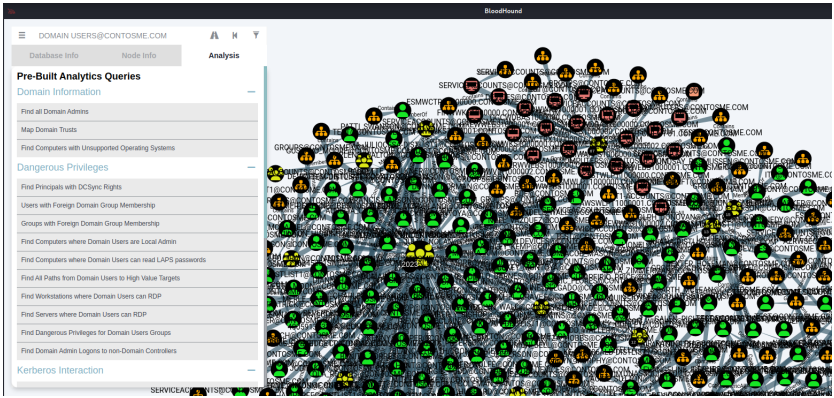




Privilege Escalation



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
  - Vorraussetzung: 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]

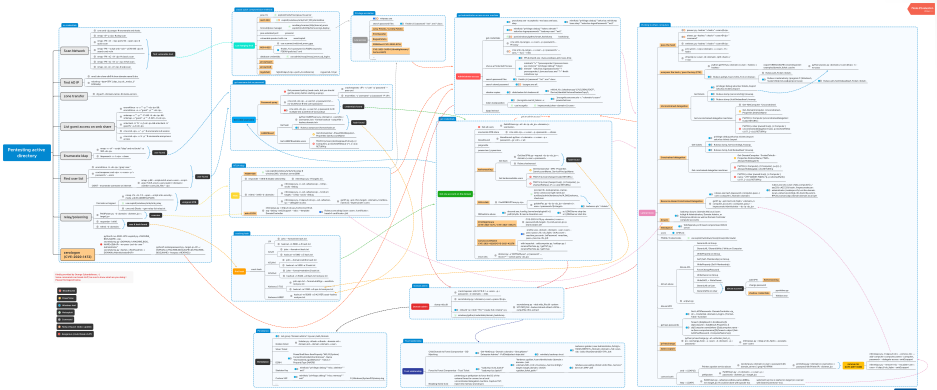
[22] https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/post/multi/manage/autoroute.md

[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



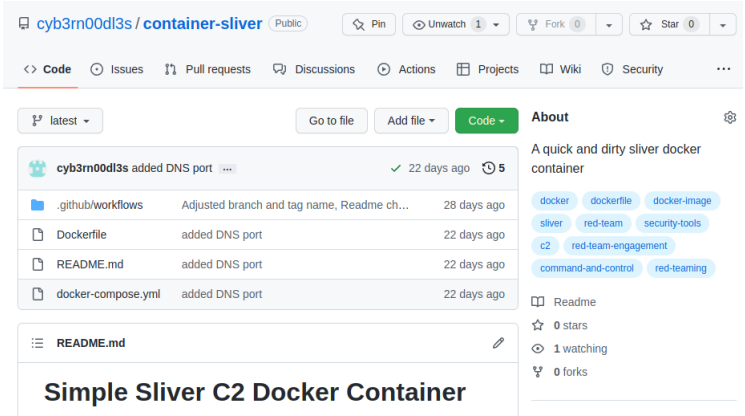
Review

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 $\Rightarrow$ Keine komplette Killchain notwendig

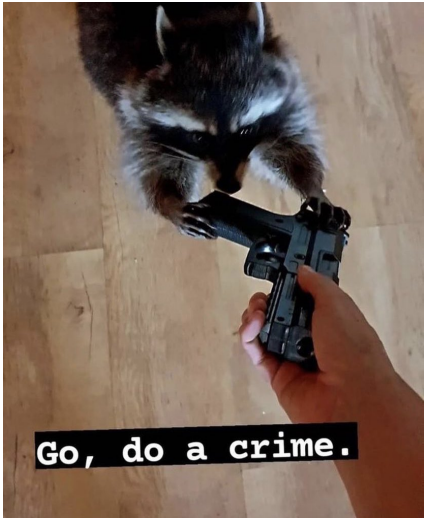
Tool Zeit!

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



Tool Zeit! (x2)

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



(nur mit Erlaubnis)