



# Hacking – Workshop

Eine technische Einführung für RZ-Personal

# Agenda

- Montag
  - Einführung, Hacking-Techniken
  - Hacking-Businessmodelle
  - ThreatModelling
  - MITRE ATT&ACK – Matrix (Basics)
  - Toolings



# Agenda

- Dienstag // Recon + Weaponizing
    - OSINT-Day
    - Showcase
    - OSINT – Day, HandsOn
- Hack your own Datacenter



# Agenda

- Mittwoch // Exploitation + Installation / C&C, Objectives
  - Einrichten im Netz
  - AD & Co
  - Priviledge Escalation
  - Vertical Movement
  - Command & Control
  - DataExfil



# Agenda

- Donnerstag
  - WebHacking
  - Social Engineering (TakeDown)
  - Physical Security
  - Wifi + Radio-Security



# Scope des Workshops

Ja:

- RZ mit extern sichtbaren Services
- Einbrüche von aussen (gezielt oder zufällig)
- Ransomware
- Linux/Unix



# Scope des Workshops

Nein:

- James Bond-Szenarien
- RAM-Module in Flüssigstickstoff
- Super-1337 APT-ThreatHunting
- gerichts feste Dokumentation / Gutachten
- Windows/AD-Fokus



# Unterlagen

- git clone

(ab Dienstag morgen)





# Fragerunde

- wie viele IPs extern erreichbar?
- wie viele Dienste nach aussen erreichbar?



# Einführung

## Definitionen

Unter Hacking versteht man den Einsatz von Technologie oder technischem Know-how zur Überwindung von Problemen oder Hindernissen.



# Einführung

- Für wen und warum

... technischen MA die Wege und Ziele von RZ-Einbrüchen (Hacking zu erklären und die Wichtigkeit und Optionen für Prävention zu verdeutlichen ...



# Einführung

## Definitionen

- BlackHat: Bad Guy, \$\$\$ oder Chaos
- White Hat: Good Guy, erlaubtes Pentesting, responsible Disclosure, Legal-Approval-Only
- Grey Hat: Good Guy, just for fun, ohne Legal-Approval



# Einführung

## Definitionen

- BlueTeam: Defense
- RedTeam: Offense
- PurpleTeam: im BlueTeam eingebettete
- nur im Enterprise-Umfeld (kein Pentest!)



# Einführung

- Angriffspunkte für Hacker
  - Physical Security (Gebäudesicherheit)
  - Systemic Attack-Surface (externe Angriffsoberfläche von IT-Systemen, Kabel und Funk)
  - Social Engineering (personelle Sicherheit)
  - Lieferketten (SolarWinds)



# Einführung

- Passwortkomplexität und Brute-Force-Angriffe auf Passwörter
- CredentialStuffing / Password Reuse
- Angriffe auf offene Datenbanken
- Angriffe auf ActiveDirectory, mimikatz
- Botnetz-Angriffe/Exploits
- DoS, DDoS, Smokescreening



# Hacking - Businessmodelle

- Ransomware / Verschlüsselung + Erpressung
- Cryptobots
- DDoS
- Auftragsarbeiten (Datenklau)
- Skiddos, politische Hintergründe
- Exkurs
- <https://zero.bs/ransomware-vs-infrastruktur-de.html>





# Ransomware

- <https://public.intel471.com/blog/revil-ransomware-interview-russian-osint-100-million/>

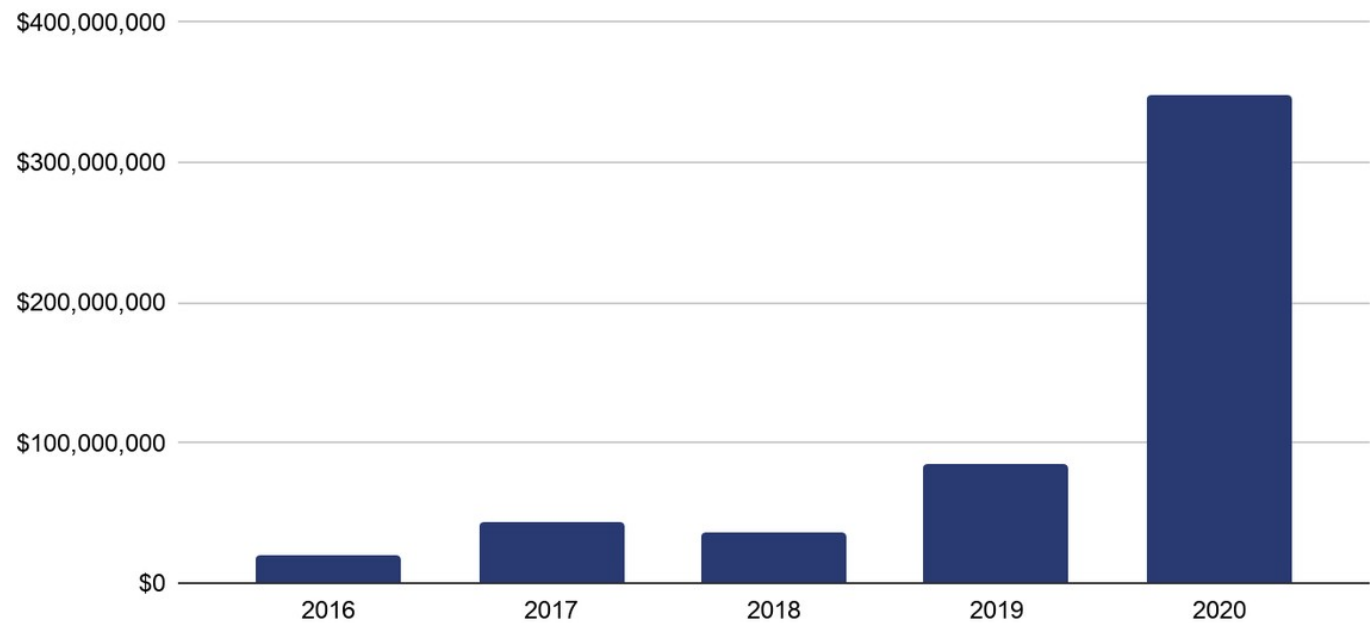
”This model has apparently led to skyrocketing profits: according to the REvil representative, one affiliate’s earnings **rose from about US \$20,000 to US \$30,000** per target with another RaaS offering **to about US \$7 million to \$8 million per target** in only six months after joining forces with REvil.”



# Ransomware

- <https://www.zdnet.com/article/ransomware-gangs-made-at-least-350-million-in-2020/>

Total value received by ransomware addresses per year, 2013 - 2020



# Ransomware

- Entrypoints:
  - Externe IT mit ungepatchte Schwachstellen neu in 2020, lukrativ, da zuhauf zu finden
  - Spam – Mails mit Anhängen (bis 2019 häufigster Weg)



# Hacking - Businessmodelle

- Angriffsoberfläche // Bedrohungslage // Exploit-Lage
- \$\$\$ makes the world go round
- Beispiele Shitrix und Cisco ASA vs BSI
- 1400 bekannte Opfer (90% der Betroffenen zahlen)



# Hacking - Businessmodelle

- Aktuell:

- <https://www.journaldemontreal.com/2020/10/29/cyberattaque-contre-le-reseau-de-la-sante-a-montreal>
- <https://www.beckershospitalreview.com/cybersecurity/oregon-hospital-shuts-down-computer-system-after-ransomware-attack-4-notes.html>
- [https://www.nbcnews.com/tech/security/cleveland-area-hospital-goes-offline-after-apparent-cyberattack-n1241408?&web\\_view=true](https://www.nbcnews.com/tech/security/cleveland-area-hospital-goes-offline-after-apparent-cyberattack-n1241408?&web_view=true)
- [https://www.nbcnews.com/tech/security/cleveland-area-hospital-goes-offline-after-apparent-cyberattack-n1241408?&web\\_view=true](https://www.nbcnews.com/tech/security/cleveland-area-hospital-goes-offline-after-apparent-cyberattack-n1241408?&web_view=true)
- [https://twitter.com/Bank\\_Security/](https://twitter.com/Bank_Security/)
- <https://twitter.com/UnderTheBreach>
- 
- Ransom-Sites



# APT



Catalin Cimpanu  
@campuscodi



FireEye has published a report today on UNC1945, a threat actor that used a Solaris zero-day to breach corporate networks

- CVE is CVE-2020-14781 (patched last month)
- Zero-day appears to have been bought off a black-market website for \$3,000

[zdnet.com/article/hacker...](https://zdnet.com/article/hacker...)



10:48 PM · Nov 2, 2020 · Twitter Web App



zeroBS  
<https://zero.bs>

# Exkurs ThreatModelling

- "Threat modeling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized. The purpose of threat modeling is to provide defenders with a systematic analysis of what controls or defenses need to be included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker."



# Exkurs ThreatModelling

- Warum ist ThreatModelling (am besten im Vorfeld) wichtig
- Begrenzen des Angriffspunkte:
  - der Heuhaufen wird signifikant kleiner
  - Die Ursachensuche wird beschleunigt
  - Die “üblichen Verdächtigen” als erstes untersucht (höhere Trefferwahrscheinlichkeit)





# Exkurs ThreatModelling

- Arbeitsweisen und Detektionswahrscheinlichkeiten von Actors gem ThreatMatrix



# Exkurs MITRE ATT&ACK - Matrix

## Phases of the Intrusion Kill Chain



# Exkurs MITRE ATT&ACK

- MITRE ATT&CK – Matrix
- <https://attack.mitre.org/>
- Attacker-Techniken und



# Exkurs Tools

- Best tool: Brain.exe && Erfahrung
- Distros:

Kali Linux

pwnPi

SigIntOS



# Exkurs Tools

- Best tool: Brain.exe && Erfahrung
- Frameworks & Tools

nuclei (recon + exploitation)

nmap et al (recon)

metasploit (exploitation & installation)

mimicatx & bloodhound && ....

cobaltstrike (post-exploitation & installation)



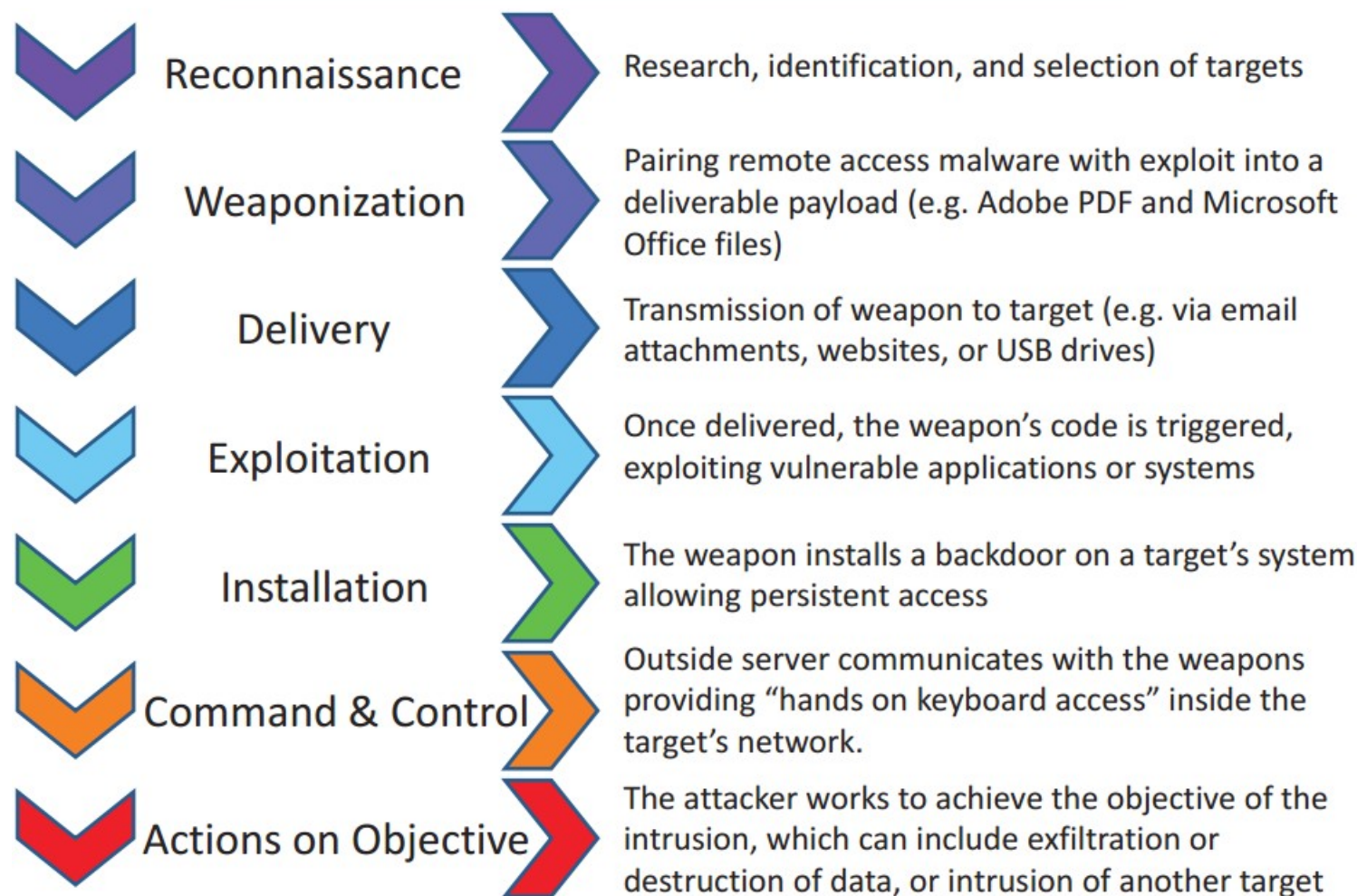
# Exkurs ThreatModelling

- Abschluß Montag / Übung (Selbstversuch)
  - ThreatModelling
  - MITRE ATT&CK
  - Einschätzung Schutzniveau



# --[ Dienstag // Recon and Weaponizing]-----

## Phases of the Intrusion Kill Chain



## --[ Dienstag // Recon, Weaponizing, Exploitation]-----

- Recon ++ OSINT

OpenSignalIntelligence / OpenSourceIntelligence

... das Sammeln und Auswerten öffentlich verfügbarer  
Daten- und Informationsquellen ...





## --[ Dienstag // Recon, Weaponizing, Exploitation]-----

- Passive, lautlose Aufklärung und Bau eines Angriffsplans
- Oceans11
- Referenzprojekt!



## --[ Dienstag // Recon, Weaponizing, Exploitation]-----

- Vom Unternehmensnamen zum Angriffsplan
- Domain → IP → RZ → Angriffsoberfläche
- Domain → Subdomains → mehr RZ → mehr Angriffsoberfläche
- Von der Angriffsoberfläche zum Exploit
- Exploits finden
- Exploits lesen



## --[ Dienstag // Recon, Weaponizing, Exploitation]-----

- Dienstag Nachmittag Übung:
  - Recon gegen die eigene Arbeitsstelle



# ---[ Mittwoch ]--Exploitation & Installation-----

- Delivery / Exploitation
- Persistenz
  - Accounts & Zugänge einrichten
  - Backdoors
  - Webshells
- Vertical movement



# ---[ Mittwoch ]--Exploitation & Installation-----

- Exploitation
  - Übung
    - F5/Citrix/Cisco
    - RCE/SessionAttacks
    - exemplarisch



# ---[ Mittwoch ]--Exploitation & Installation-----

- Installation & Persistenz
  - How to survive a Reboot
  - Backdoors und Account-Takeover  
VPN-Gateway-attacks  
mimikatz, PW-cracking
  - AD-Hacking & DC-Takeover
  - Avg 200 Tage im Netz, unerkannt



# ---[ Mittwoch ]--Exploitation & Installation-----

- Privilege escalation & Vertical movement
  - Internal Phishing
  - DNS-takeover
  - Arp-Poisoning
  - Passives Networksniffing
  - Mapping the Network-Layout
  - Datastore



# ---[ Mittwoch ]--Exploitation & Installation-----

- Privilege escalation & Vertical movement
  - SecurityControls
  - Testballons





# ---[ Donnerstag ]-- Backchannels-----

- Command&Control / Backchannels
  - ReverseShell/Payloads
  - TCP direct
  - Tunneling
  - DNSTunnel (Übung)



# ---[ Donnerstag ]--Goodies

- Physical Security
  - Devices: Bashbunny
  - Office: MAC, NAC, Whitelisting
  - Building: AccessControl
- Social Engineering (Takedown)
- Wifi and Radio



# Toolings / Distributionen

- REMnux
- Kali
- GRML



# Testboxen & Dojos

- OverTheWire
- HackTheBox
- CompassSecurity (EU Hacking Challenge)

