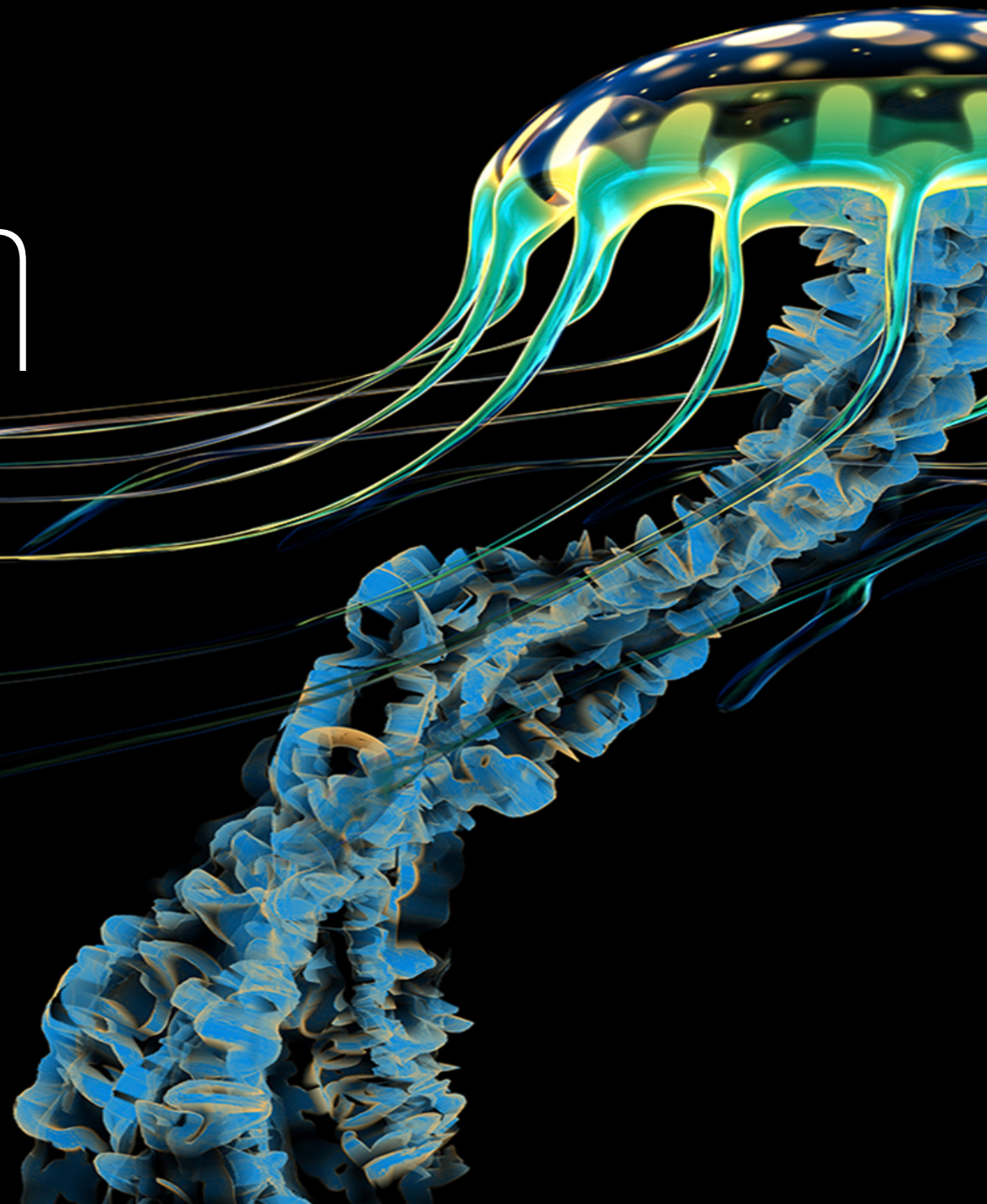
Angriffssimulation 2017

Ein Einblick in die Red Teaming Praxis

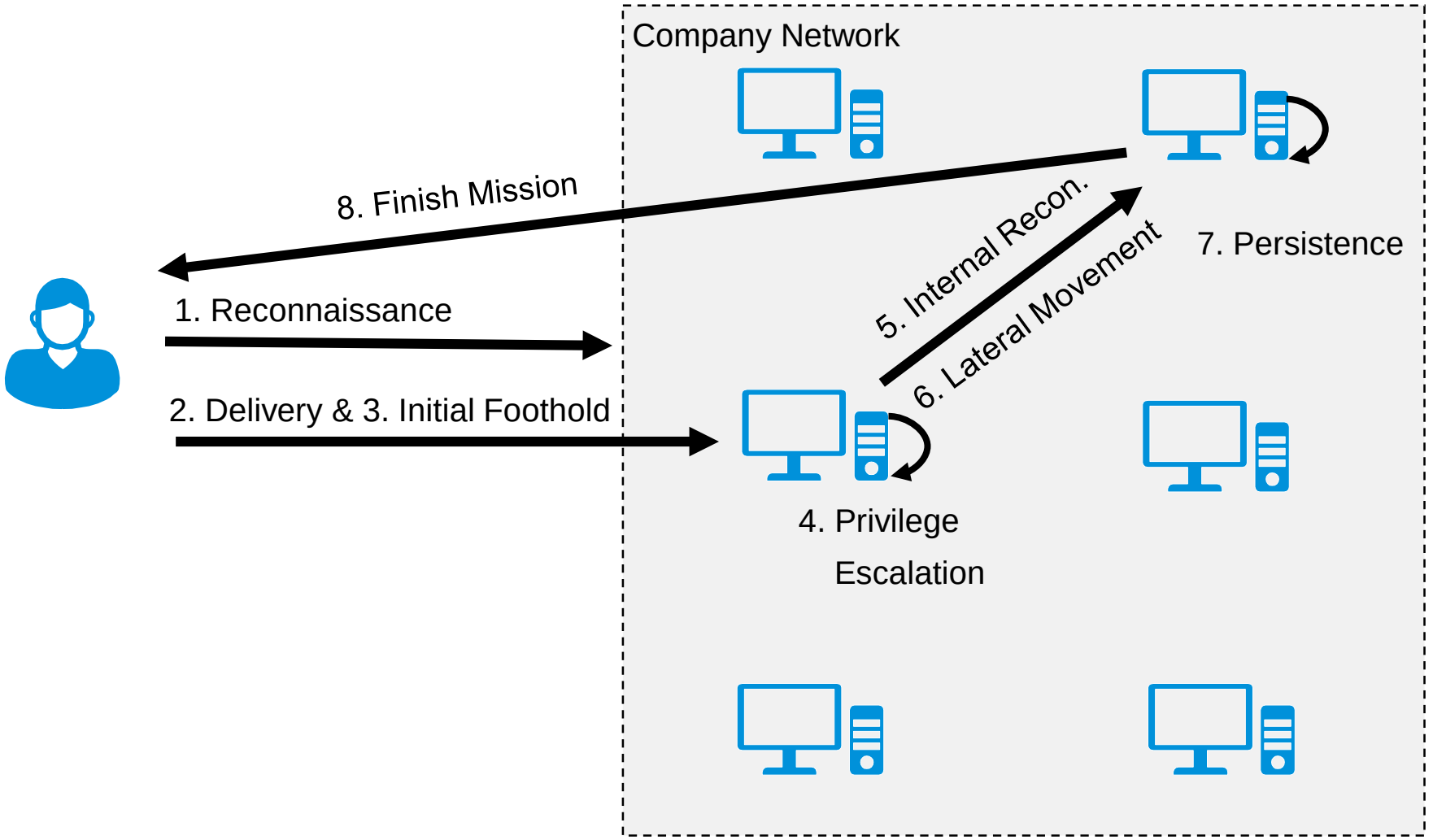


Digitalisierung von Schadsoftware

Vergleich Pentesting & Red Teaming

Penetration Testing		Red Teaming
Überblick über Schwachstellen	Ziel	**Test der Robustheit gegen realistische Angriffe**
Definiertes Subset	Umfang	**Realistische Angriffspfade**
Fokus auf präventiven Kontrollen	Getestete Kontrollen	**Fokus auf Erkennung und Reaktion**
Fokus auf Effizienz	Testmethode	**Fokus auf realistischer Simulation**
Reconnaissance , Scanning, Enumeration,…	Testtechniken	**Angreifer Werkzeuge, Methoden, Techniken**
Sehr limitiert	Post-Exploitation	**Fokus auf „Kronjuwelen“**

Schematische Vorgangsweise gezielter Angriffe

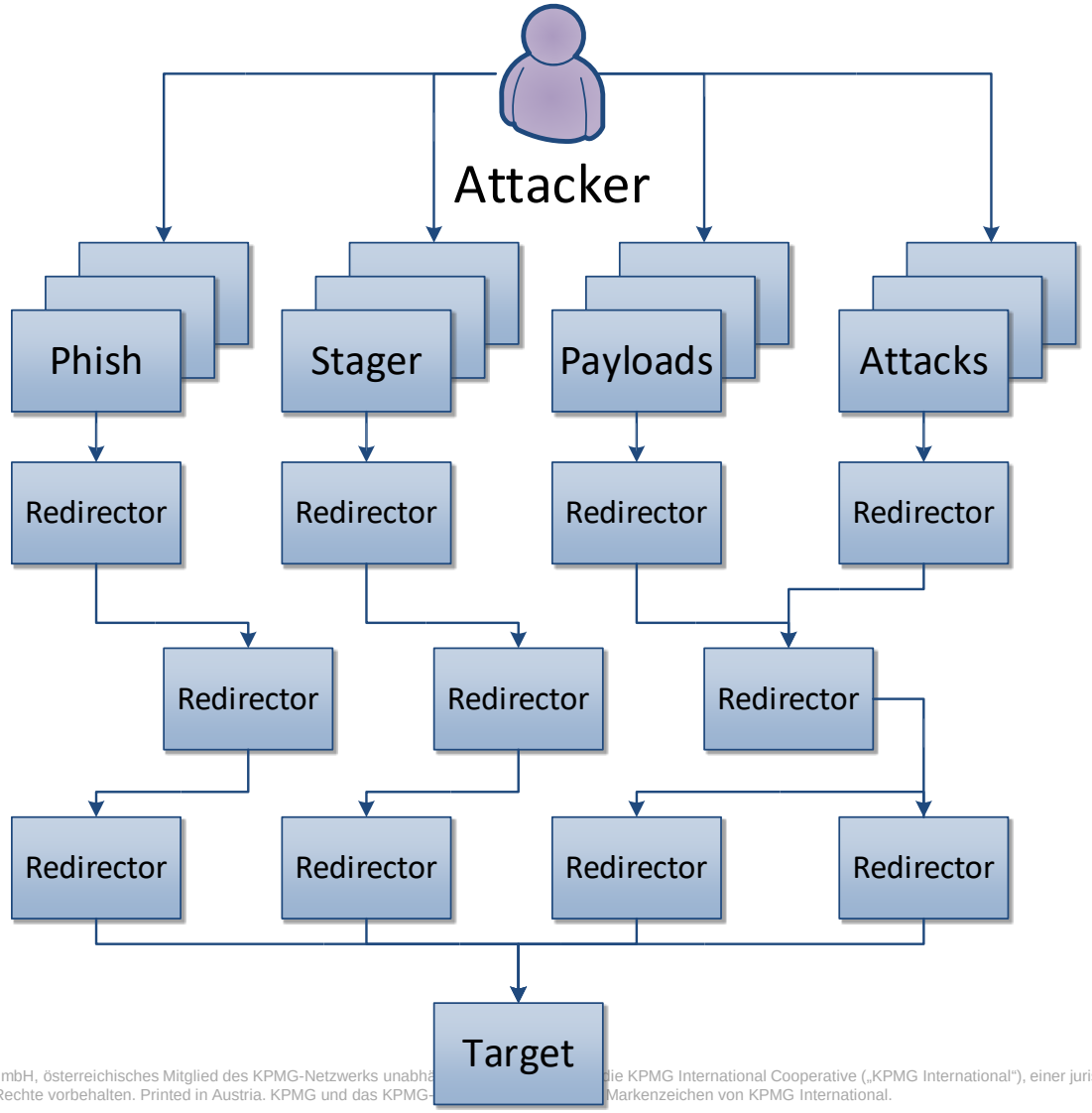


Mitre ATT&CK Framework

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Application Shimming	Automated Collection	Data Compressed	Communication Through Removable Media
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Exploitation of Vulnerability	Command-Line Interface	Clipboard Data	Data Encrypted	Connection Proxy
Application Shimming	Application Shimming	Clear Command History	Create Account	Network Service Scanning	Logon Scripts	Execution through API	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Authentication Package	Bypass User Account Control	Code Signing	Credential Dumping	Network Share Discovery	Pass the Hash	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Peripheral Device Discovery	Pass the Ticket	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Permission Groups Discovery	Remote Desktop Protocol	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Component Firmware	Dylib Hijacking	DLL Injection	Input Capture	Process Discovery	Remote File Copy	Launchctl	Email Collection	Exfiltration Over Physical Medium	Fallback Channels
Component Object Model Hijacking	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Prompt	Query Registry	Remote Services	PowerShell	Input Capture	Scheduled Transfer	Multi-Stage Channels
Cron Job	File System Permissions Weakness	DLL Side-Loading	Keychain	Remote System Discovery	Replication Through Removable Media	Process Hollowing	Screen Capture		Multiband Communication
DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	Network Sniffing	Security Software Discovery	Shared Webroot	Regsvcs/Regasm	Video Capture		Multilayer Encryption
Dylib Hijacking	Local Port Monitor	Disabling Security Tools	Private Keys	System Information Discovery	Taint Shared Content	Regsvr32			Remote File Copy
External Remote Services	New Service	Exploitation of Vulnerability	Securityd Memory	System Network Configuration Discovery	Third-party Software	Rundll32			Standard Application Layer Protocol
File System Permissions Weakness	Path Interception	File Deletion	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Scheduled Task			Standard Cryptographic Protocol
Hidden Files and Directories	Plist Modification	File System Logical Offsets		System Owner/User Discovery	Windows Remote Management	Scripting			Standard Non-Application Layer Protocol
Hypervisor	Scheduled Task	Gatekeeper Bypass		System Service Discovery		Service Execution			Uncommonly Used Port
LC_LOAD_DYLIB Addition	Service Registry Permissions Weakness	HISTCONTROL		System Time Discovery		Source			Web Service
Launch Agent	Setuid and Setgid	Hidden Files and Directories				Space after Filename			
Launch Daemon	Startup Items	Hidden Users				Third-party Software			
Launchctl	Sudo	Hidden Window				Trap			
Local Port Monitor	Valid Accounts	Indicator Blocking				Trusted Developer Utilities			
Login Item	Web Shell	Indicator Removal from Tools				Windows Management Instrumentation			
Logon Scripts		Indicator Removal on Host				Windows Remote Management			
Modify Existing Service		Install Root Certificate							
Netsh Helper DLL		InstallUtil							
New Service		LC_MAIN Hijacking							
Office Application Startup		Launchctl							
Path Interception		Masquerading							
Plist Modification		Modify Registry							
Rc.common		NTFS Extended Attributes							
Re-opened Applications		Network Share Connection Removal							
Redundant Access		Obfuscated Files or Information							
Registry Run Keys / Start Folder		Plist Modification							
Scheduled Task		Process Hollowing							
Security Support Provider		Redundant Access							
Service Registry Permissions Weakness		Regsvcs/Regasm							
Shortcut Modification		Regsvr32							
Startup Items		Rootkit							
System Firmware		Rundll32							
Trap		Scripting							
Valid Accounts		Software Packing							
Web Shell		Space after Filename							
Windows Management Instrumentation Event Subscription		Timestomp							
Winlogon Helper DLL		Trusted Developer Utilities							
		Valid Accounts							

Tarnen & Täuschen

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission



Phishing

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission

Frohe Weihnachten von Ihrer Universität! Posteingang x severin.winkler@gmx.at x

Alumnimap <alumnimap@univie.ac.at> Abbestellen 21.12.16
an Alumnimap

Sehr geehrte AbsolventInnen,
Sie haben Ihr Studium an der **Universität Wien** erfolgreich abgeschlossen und seither viele wichtige Erfahrungen gesammelt. Heute möchten wir Sie zu einer spannenden Initiative einladen:

Werden Sie Teil der Online-Community von Uni-Wien-AbsolventInnen auf der **Alumni Map** der Universität Wien. Sie gehören „dazu“, werden immer wieder über interessante Entwicklungen an der Uni Wien informiert und können auch gewinnen: Sobald wir 7.500 Einträge erreicht haben, verlosen wir **3 iPad Air** (aktuell sind es ca. 7.200 Einträge).

Was müssen Sie tun? Registrieren Sie sich **so rasch wie möglich** auf der Alumni Map der Uni Wien – und Sie nehmen an der Verlosung teil. Hier geht’s zur Alumni Map: **alumnimap.univie.ac.at**

Wir freuen uns sehr, wenn Sie sich eintragen und damit als AbsolventInnen der Universität Wien sichtbar werden!

Mit den besten Wünschen für ein frohes Weihnachtsfest und herzlichen Grüßen,

ao. Univ.-Prof. Mag. Dr. Christa Schnabl
Vizerektorin der Universität Wien

PS: Sollten Sie sich bereits eingetragen haben, bedanken wir uns herzlich - Sie brauchen nichts weiter zu tun und nehmen automatisch an der Verlosung teil.

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission

Delivery

- **Klassische Angriffe über die externe Infrastruktur**
- **Phishing**
  - Spear Phishing
  - Whale Phishing
  - CEO Fraud
- **USB Sticks**
  - Spezial-“Sticks“ (RubberDucky, USB Armory, etc.)
  - Normale „Sticks“ mit Macro, PDF, …
- **Physisches Social Engineering (Ziel: Netzwerkzugriff)**
  - Keylogger mit WLAN Modul
- **Telefonanrufe**

Codeausführung

- **Office Macro**
  - *bilanz_2017.xls*
  - Auch Exotische Dateitypen: Microsoft Publisher
- **HTML Application**
  - *bilanz_2017.hta*
  - Datei die (nur) vom Internet Explorer ausgeführt wird.
- **Windows Dropper**
  - *bilanz_2017.pdf.exe*
- **Java Applet Angriffe**
  - *bilanz_interaktiv_2017.jar*
    - Java < 2014

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission

Kommunikation nach außen

- Verwendung vorhandener Protokolle für Kontrollkanal (C2)
  - HTTPS
  - HTTP
  - DNS
  - SMB
  - IRC
  - FTP
  - Britney Spears Instagram Account
  - …

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission

Privilege Escalation

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission

Ausnutzen von Schwachstellen oder Fehlkonfigurationen um volle Systemrechte zu erlangen.

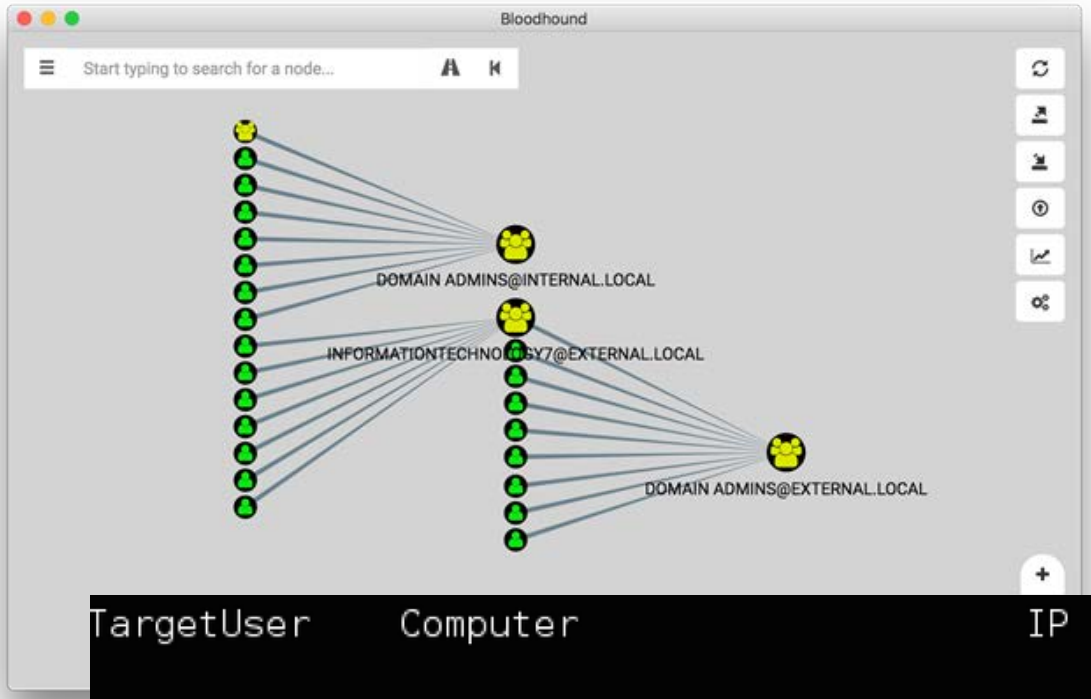
- Windows Services
- Scheduled Tasks
- Umgehung von UAC
- Mimikatz
- Group Policy Preferences (GGP)
- Wiederverwendung von Zugangsdaten
- …

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission

Interne Reconnaissance

Analyse von Hosts + Vertrauensbeziehungen

„Admin Hunting“




```
TargetUser    Computer                        IP              SessionFrom

----------    --------                        --              -----------
Administrator WINDOWS3.dev.testlab.local      192.168.52.205
Administrator SECONDARY.dev.testlab.local     192.168.52.105 192.168.52.206
Administrator SECONDARY.dev.testlab.local     192.168.52.105 192.168.52.205
```

Lateral Movement - Beispiel

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission

1.)

Finde alle *.exe Dateien auf allen Dateiservern die in den letzten Tagen geschrieben worden sind.

```
Invoke-ShareFinder -CheckShareAccess
Find-InterestingFile -FreshEXEs –CheckWriteAccess
```

2.)

„Trojanisiere“ diese Dateien (bzw. einzelne)

```
./backdoor.py -f putty.exe […] -s reverse_shell_tcp
```

3.)

Kopiere die Dateien zurück

```
Copy-ClonedFile
```

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission

Persistence

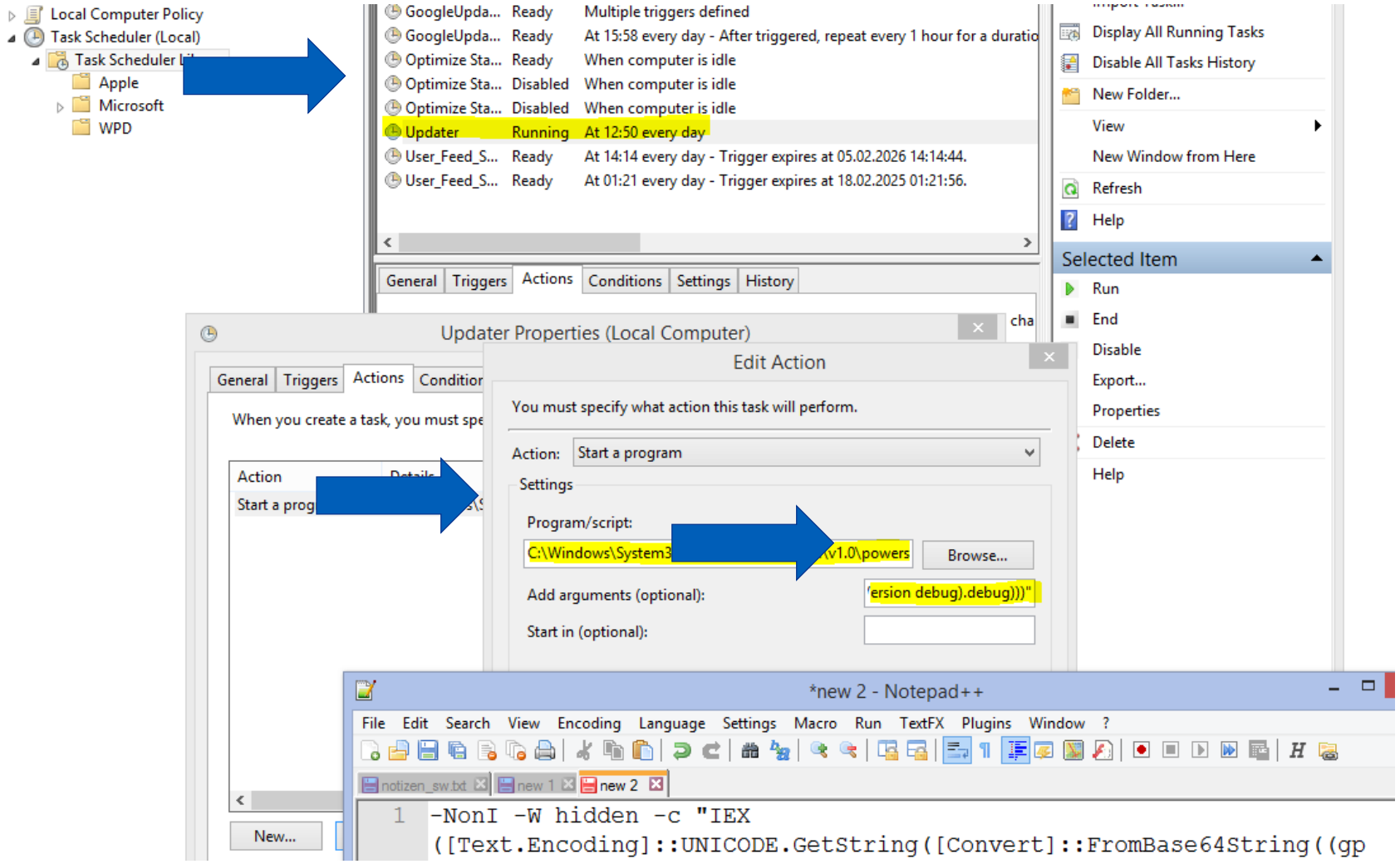
Überlebe den Neustart!

- Keine Persistenz ohne Schreibzugriff auf Platte bekannt!

- Auslösung des Payloads beim Login
- Aufgabenplanung (Scheduled Tasks)
- Windows Services
- WMI (Windows Management Interface)
- …

Persistence

1	Reconnaissance
2	Delivery
3	Initial Foothold
4	Privilege Esc.
5	Internal Recon.
6	Lateral Movement
7	Persistence
8	Finish Mission



Risiken beim Red Teaming

- **Unterschiedliche Zielsetzungen**
  - CEO will Pentest, CFO will Social Engineering, durchgeführt wird Red Teaming
- **Unklare Kommunikation**
  - Was wird abgestimmt und was nicht?
  - C2 Verbindungen nicht (mit Betriebsrat) abgestimmt.
- **Datenschutz**
  - Was passiert wenn ein Mitarbeiter USB Sticks privat ansteckt?
- **Scope Creep**
  - Ab wann wird aus Red ein Blue Teaming?

Take Aways - Red Teaming

- **realistisches** Bild
- **aufwändiger** als klassischer Pentest
- **längere Durchlaufzeit**
- **Abstimmungsaufwand**

- Äpfel & Birnen:
  - Pentest
  - Pentest mit allen Delivery Methoden
  - Red Teaming
  - Purple Teaming

Fragen?


Severin Winkler

Manager
Cyber Security / IT Advisory

KPMG Security Services GmbH
Porzellangasse 51
1090 Wien

M +43 664 820 24 24
severinwinkler@kpmg.at
kpmg.at

Referenzen: APT Modelle

Raytheon:

https://krypt3ia.files.wordpress.com/2012/02/apttacticsraytheon.jpg

Symantec:

http://www.symantec.com/content/en/us/enterprise/images/b-apt_infographic.jpg

Wikipedia:

https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

Referenzen

PowerSploit

https://github.com/PowerShellMafia/PowerSploit.git

Empire

https://github.com/PowerShellEmpire/Empire

https://enigma0x3.net/2015/08/26/empire-tips-and-tricks/

Cobalt Strike

https://www.cobaltstrike.com

Nishang

https://github.com/samratashok/nishang

http://resources.infosecinstitute.com/nishang-a-post-exploitation-framework/

Veil Framework

https://www.veil-framework.com/

Persistence options with Empire

http://www.harmj0y.net/blog/empire/nothing-lasts-forever-persistence-with-empire/

Mitre ATT&CK Framework

https://attack.mitre.org