DIHSÜD
Digital Innovation Hub

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Workshop Hacking Basics

08.05.2023 - Seifenfabrik

Dr. Klaus Gebeshuber
klaus.gebeshuber@fh-joanneum.at
Thomas Strametz, MSc
thomas.strametz@fh-joanneum.at

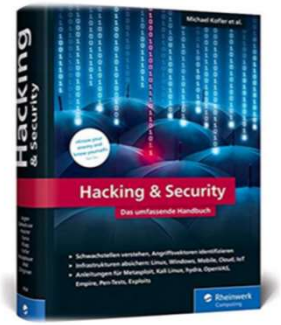
FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

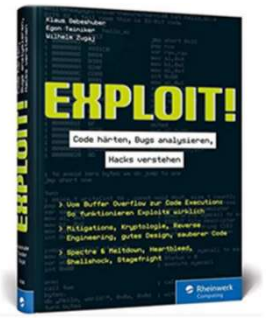
Klaus Gebeshuber

- **Who am I**
  - Married, 2 Children (21, 24)
  - I like: Family, Mountain Biking, Skiing tours, Fire Brigade, IT-Security
  - Study of Electronic Engineering / Computer Science
  - 15 years Industrial Software Development / Warehouse Logistics

- **Lectures @ FH JOANNEUM**
  - Network Technologies, Basic/Mobile Network Security
  - IT-Security
  - Ethical Hacking, Advanced System Exploitation

- **Research Activities**
  - Industrial Penetration Testing
  - Wireless Security
  - 0day hunting, Bug hunting, Bug Bounty Automation





- **Industrial Certifications**
  - OSCP, OSCE, CISSP, OSWP, CCNA, eCPPT, CSM, eMAPT

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Thomas Strametz

- Education
- 2011 – 2016 HTBLA Kaindorf Informatik
- 2017 – 2020 BSc in Engineering (ITM @ FHJ)
- 2020 – 2022 MSc in Engineering (IT & Mobile Security @ FHJ)

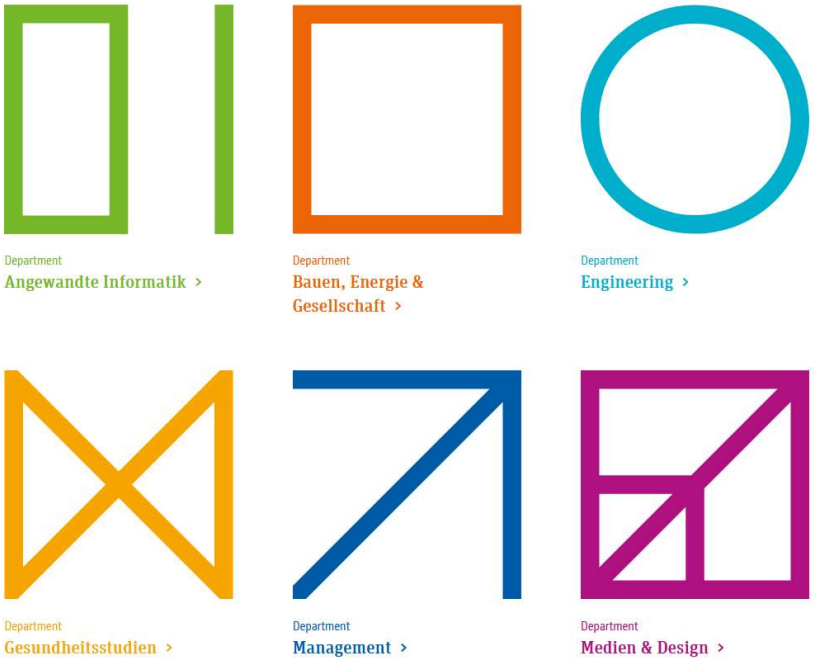
- Work Experience
- 2017 – 2019 SAP Cloud Development (B4B Solutions GmbH)
- 2019 – now WiMa @ FHJ

- Contact
- Teams
- thomas.strametz2@fh-joanneum.at
- K.WS46a.123

FH JOANNEUM

Institut Software Design und Security

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security



Department
Angewandte Informatik ›

Bachelorstudiengänge

Gesundheitsinformatik / eHealth
Vollzeit / Graz

Mobile Software Development
Dual / Kapfenberg

Software Design & Cloud Computing
Vollzeit / Kapfenberg

Software Design & Cloud Computing
Berufsbegleitend / Kapfenberg

Wirtschaftsinformatik
Vollzeit / Graz

Masterstudiengänge

Data Science and Artificial Intelligence
Berufsermöglichend / Graz

eHealth
Berufsermöglichend / Graz

IT & Mobile Security
Berufsbegleitend / Kapfenberg

IT Architecture
Berufsermöglichend / Graz

IT-Recht & Management
Berufsbegleitend / Kapfenberg

Software and Digital Experience Engineering
Berufsermöglichend / Graz

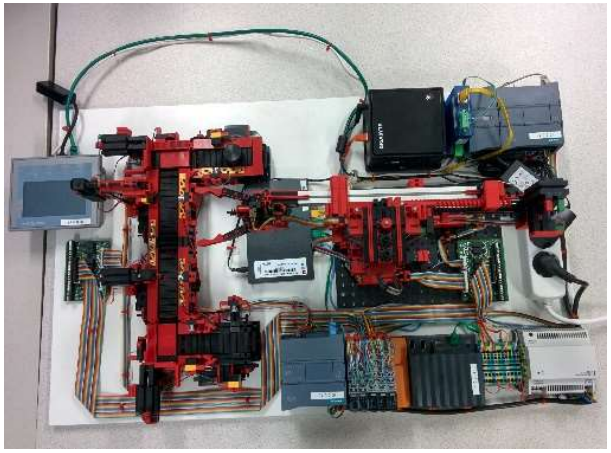
FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Security Infrastruktur

Security Lab

Password Cracker

ICS Honeypot



FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Security – Schwerpunkte im Studium

- **Bachelor Studiengänge 180 ECTS**
  - Software Design & Cloud Computing Vollzeit / berufsbegleitend
  - Mobile Software Development Vollzeit / dual
  - IT-Security Basisausbildung im 5. bzw. 6. Semester

- **Master – IT & Mobile Security - berufsbegleitend 120 ECTS**
  - Secure Software Development/Design, Mobile Security
  - Cryptography, Database Security, Network Security
  - Ethical Hacking, Advanced System Exploitation
  - Operating System Security
  - Secure Server Environments, Cloud Computing
  - Hardware Security, Embedded Systems
  - Security Management

Berufsfelder unserer AbsolventInnen ...

Penetration Tester

Secure Software Developer

CISO

Threat Hunter

/itkapfenberg /itkapfenberg

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Agenda

- 13.00 - 13.30 Infrastruktur
- 13.30 - 14.00 Network – Discovery
- 14.00 - 14.30 Network – Exploitation
- 14.30 - 15.00 Public Exploits
- 15.00 - 15.30 Web Hacking
- 15.30 - 16.00 Windows Domain Attacks

FH JOANNEUM
University of Applied Sciences
IT & Mobile Security

Infrastruktur

- WLAN
  - SSID: Pen-Test-Training-1
  - Password: pentest12345

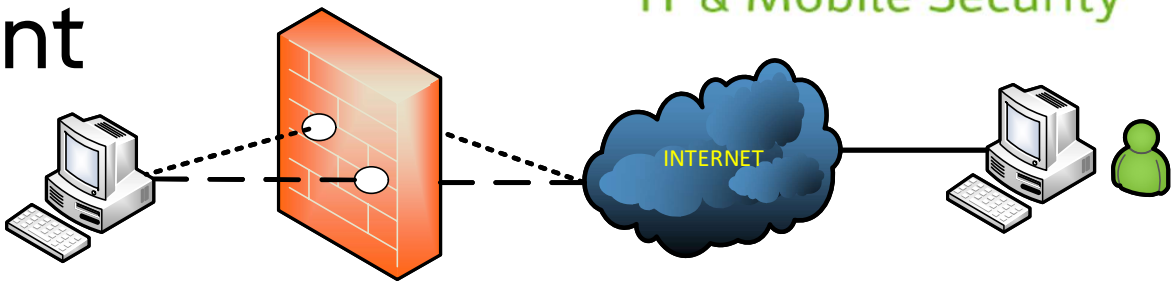
- KALI Linux
  - IP: 192.168.0.5
  - SSH
  - User: hacker1 – hacker24
  - Password: ???

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Windows Domain Attacks

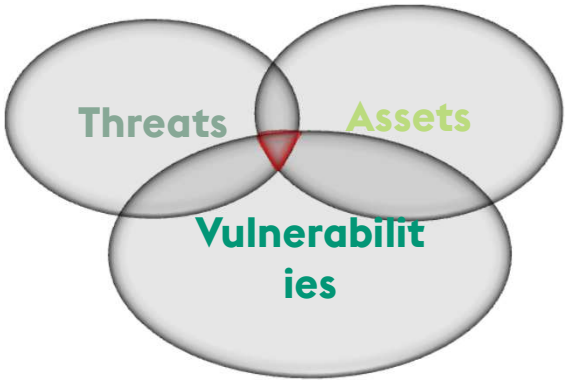
FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Vulnerability Assessment



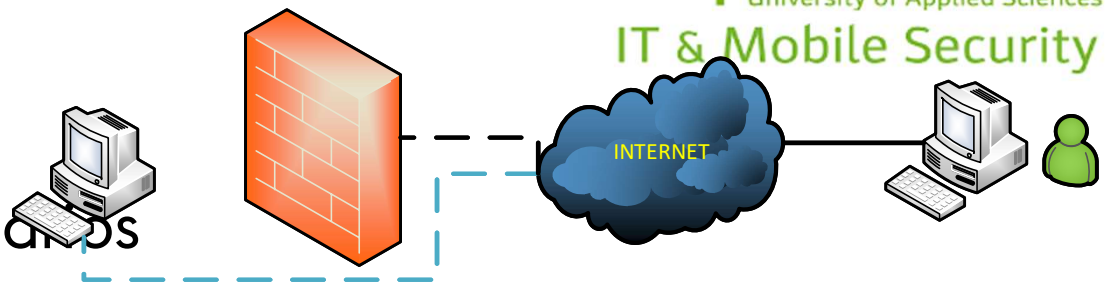
- Beschränkter Testzeitraum
- Viele Schwachstellen finden
- Automatisierte Vulnerability Scanner
- Test in die Breite
- Unterschiedliche Angriffsvektoren
- Analyse von Individual Systemen

➔ Umfangreiches Bild der Lage im Netzwerk



FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Penetration Test

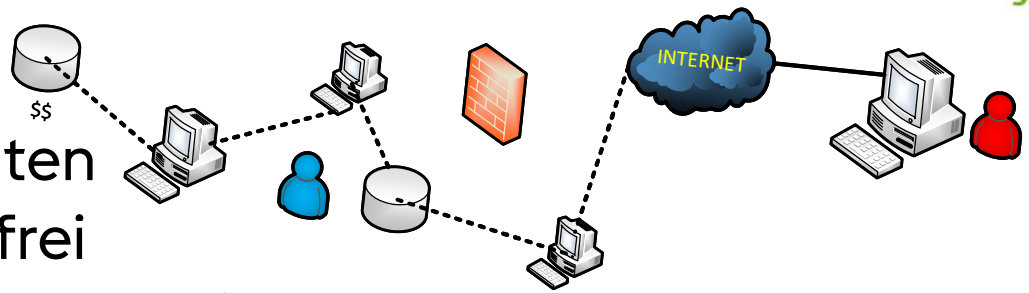


- Definition eines Worst-Case Szenarios
- Beschränkter Testzeitraum
- Automatisierte Tests, hoher manueller Anteil
- Scan in die Tiefe
- Suche nach neuen, unbekannten Schwachstellen

➔ Überprüfung bestehender Sicherheitsmaßnahmen

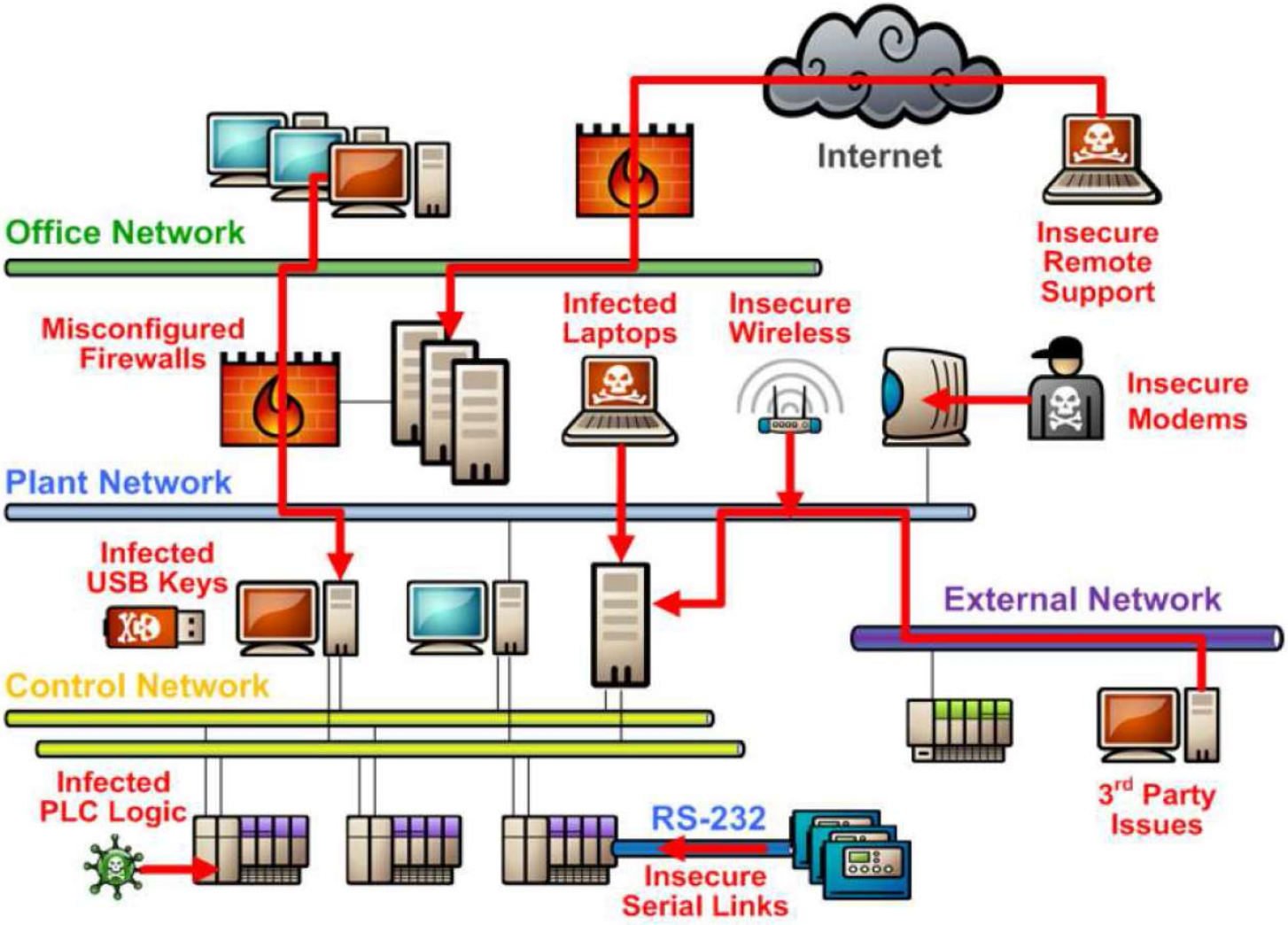
FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Red Team Assessment

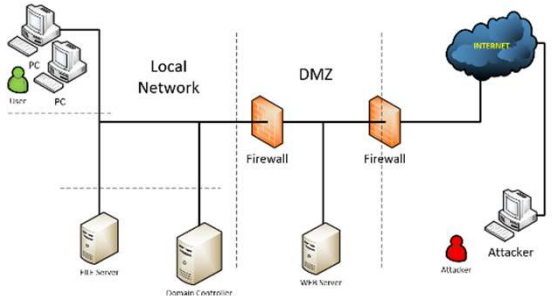


- Ziel z.B. Zugriff auf vertrauliche Daten
- Wahl der Waffen und der Wege ist frei
- Suche nach vielen Zugangspunkten zum Ziel
- Realistisches Szenario
- Training des Blue Teams in eigenen Umgebung
- Aktivitäten unter dem Radar

➔ Überprüfung des gesamten Sicherheitskonzeptes



FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

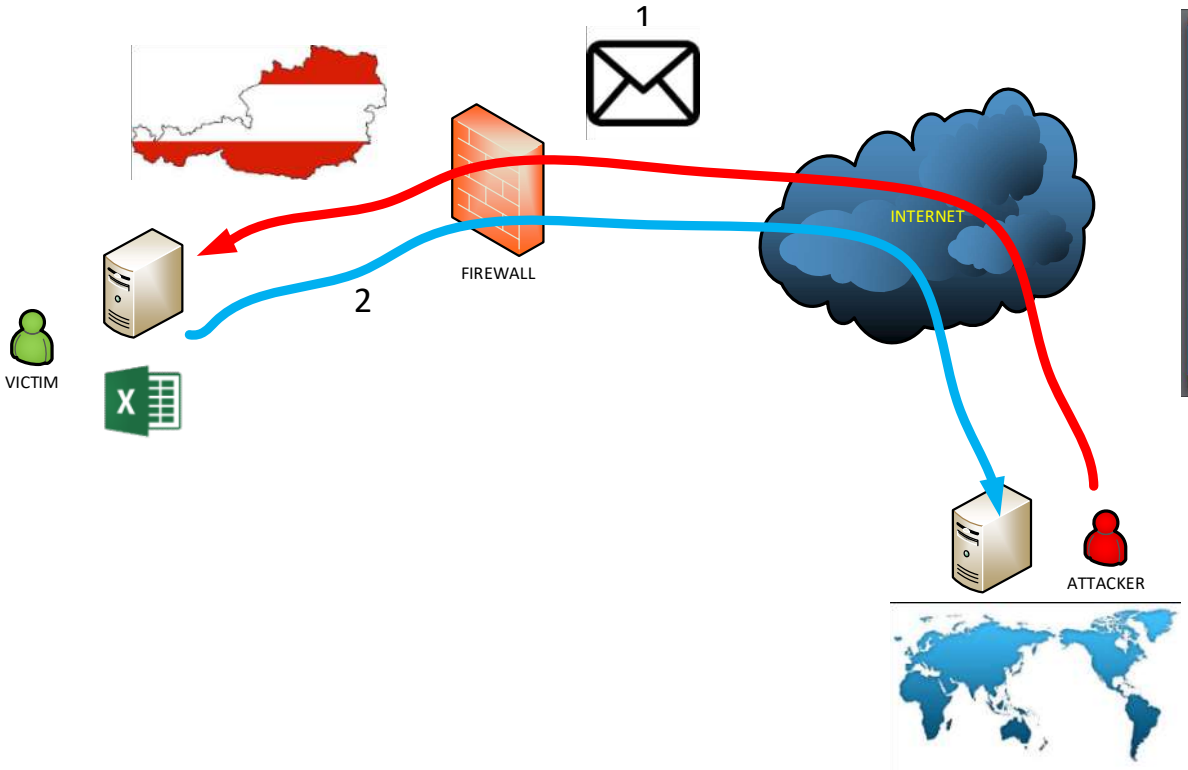


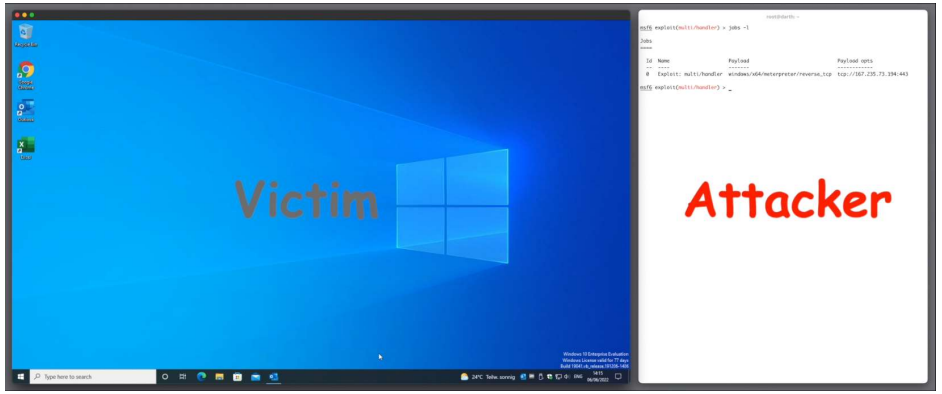
*Initial Access
*Privilege Escalation
Persistence
*Lateral Movement
*Exploitation
Data Exfiltration
Hide Tracks

https://www.tofinosecurity.com/sites/default/files/common/white-papers/Using-ISA_IEC-62443-Standards-WP-v1.2%20(May%2020

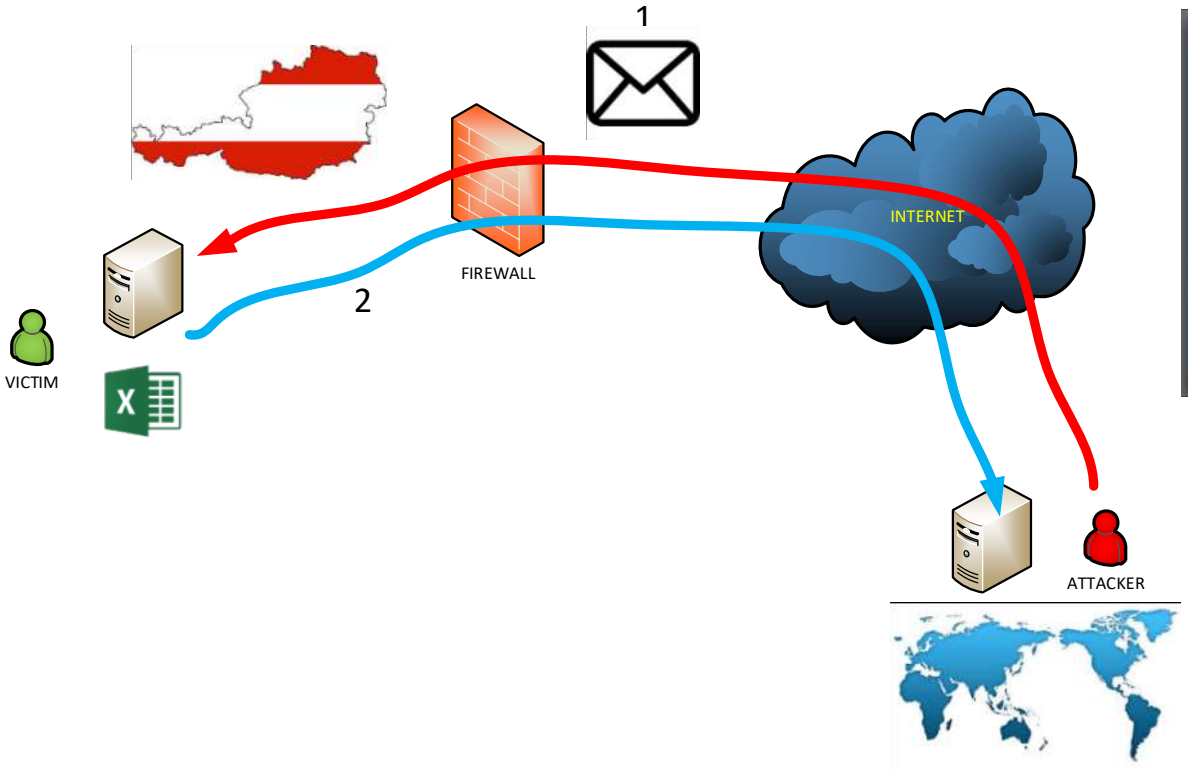
FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

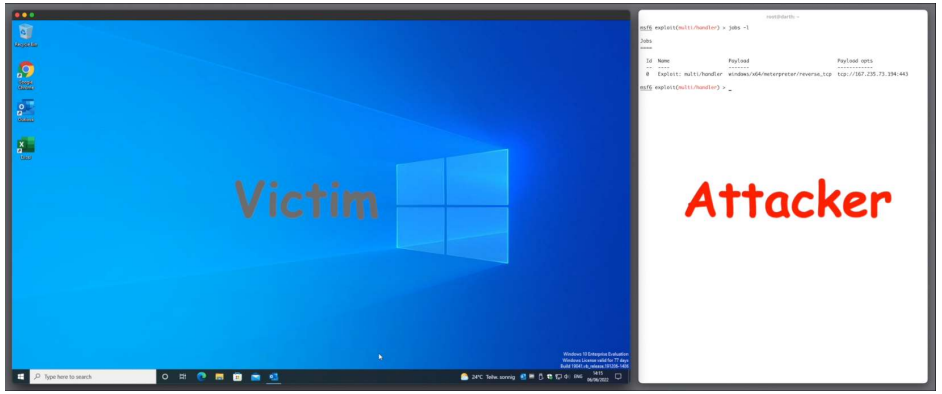
Initial infection



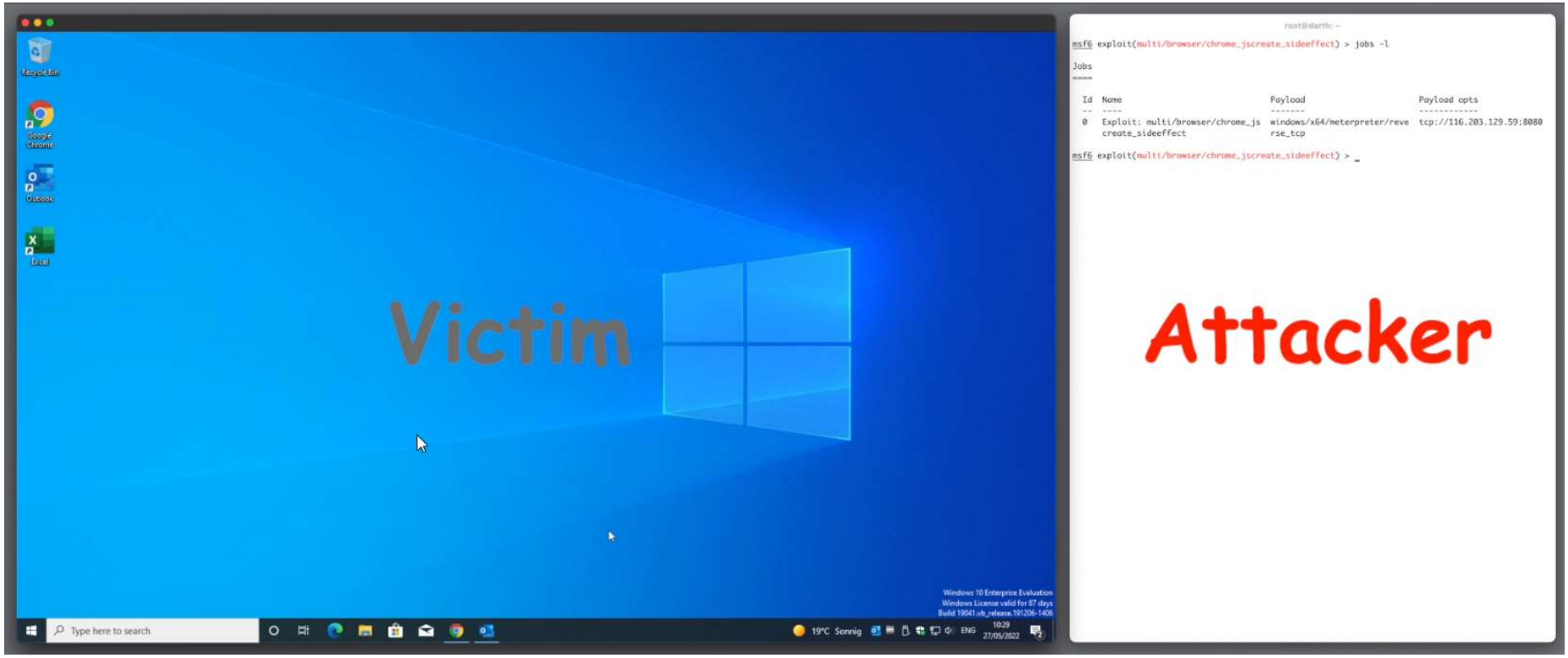


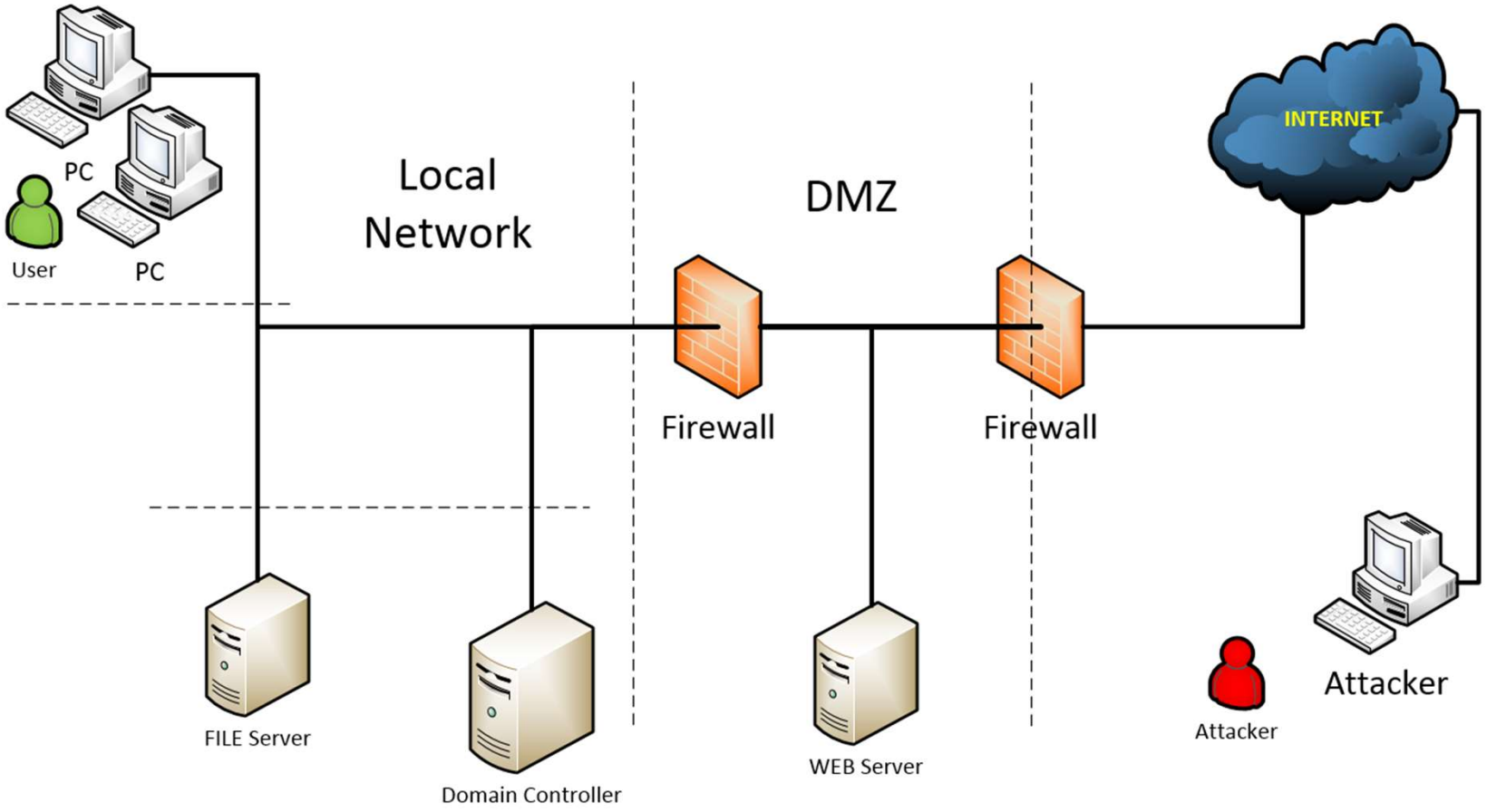
Initial infection

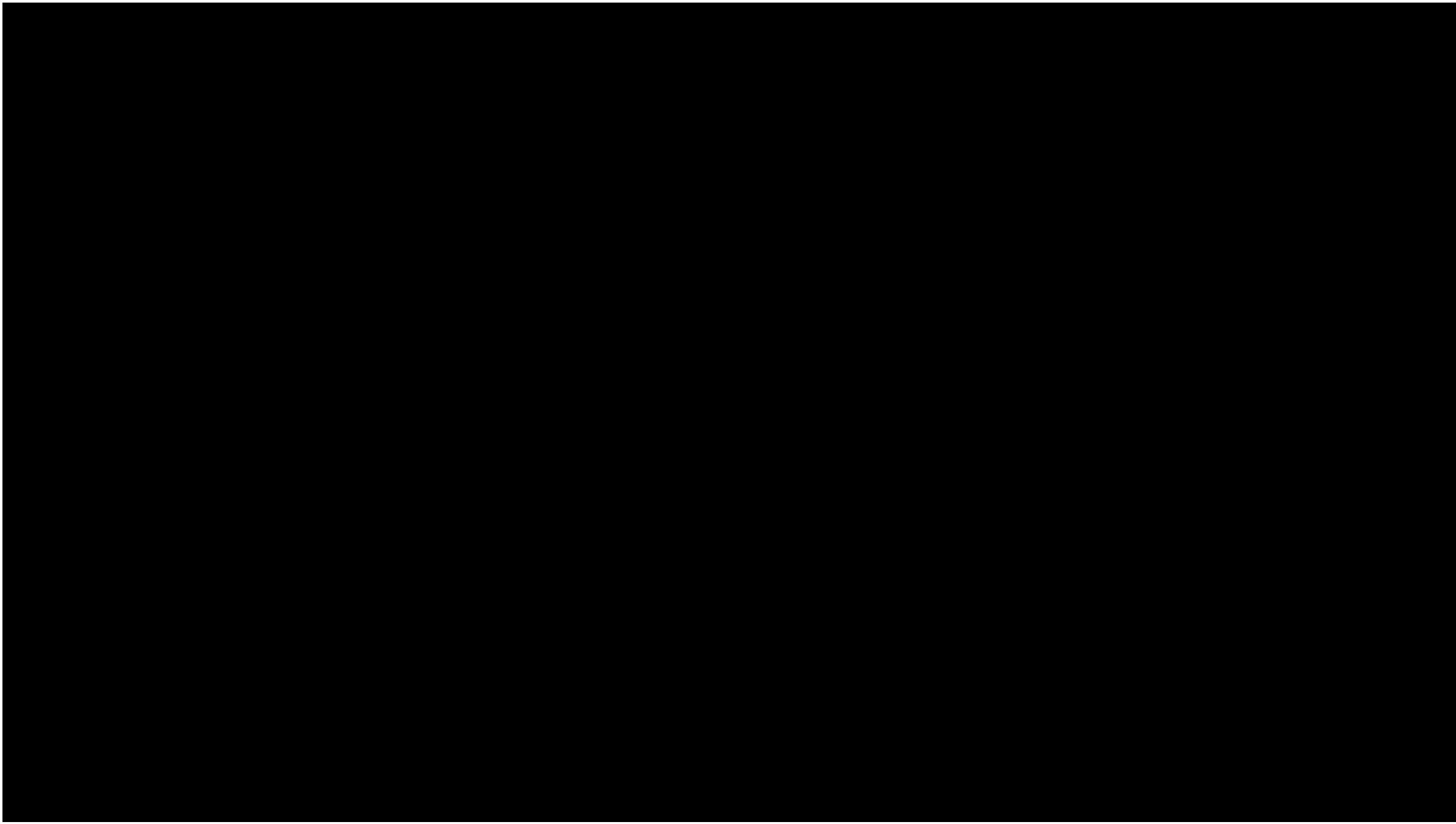




Phishing – Click on a malicious link




PC
User
PC
Local
Network
DMZ
INTERNET
Firewall
Firewall
FILE Server
Domain Controller
WEB Server
Attacker
Attacker



FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Gängige Schwachstellen in Unternehmensnetzwerken

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Netzwerk Zugriff (1)

- Physischer Zugang ohne Einschränkungen
  - Jede Netzwerkdose aktiv, IP-Adresse via DHCP, direkter Zugang ins Internet
  - 802.1X – Fehlkonfiguration – Standard VLAN - Informationsquelle
  - 802.1X – Bypass, Mac Datenbank auslesbar

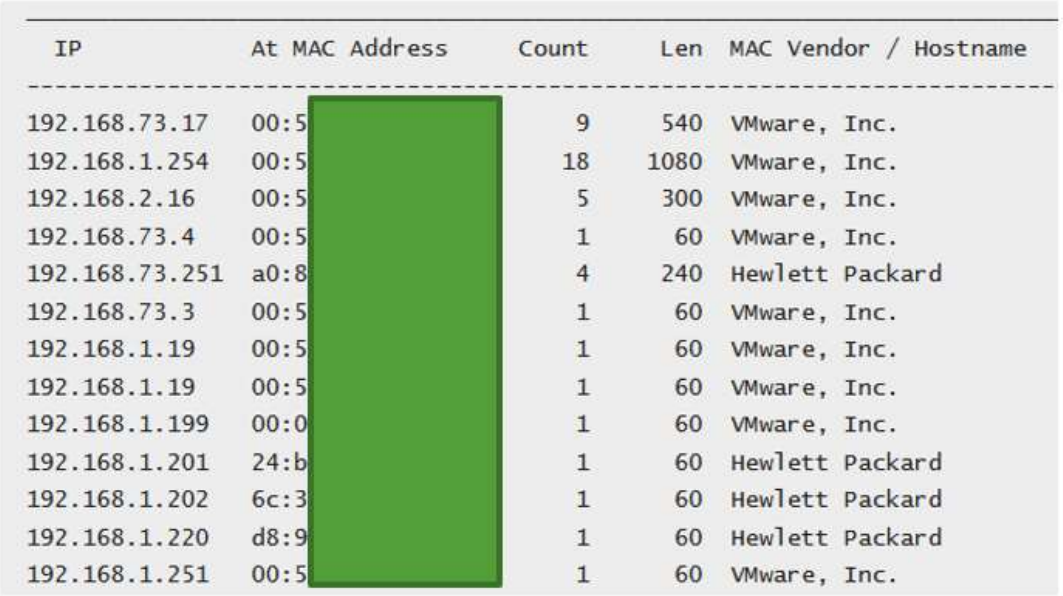
- Gäste WLAN
  - Verbindung zum internen Netz
  - Offen, kein Passwort
  - Statisches Passwort

- Internet Zugang beschränkt
  - Blockiert – via HTTP Proxy
  - ping erlaubt – Tunnel über ICMP
  - DNS erlaubt – Tunnel über DNS

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Netzwerk Zugriff (2)

- Unbekannte Geräte
  - Falsche/Standard IP Konfiguration
  - Layer 2 – Netzwerkscan
- Dual Homed
  - Geräte mit zwei Netzwerk-Karten
  - Firewall Bypass
- Keine Netzwerk Segmentierung
  - Office → Produktion
- Design Fehler – VLAN?
  - Layer 2 vs. Layer 3 Trennung
- Cisco Dynamic Trunking Protokoll
  - Zugriff in alle VLANs
- WLAN
  - WPA-2 Numerisches Passwort, WEP



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.73.17	00:5	9	540	VMware, Inc.
192.168.1.254	00:5	18	1080	VMware, Inc.
192.168.2.16	00:5	5	300	VMware, Inc.
192.168.73.4	00:5	1	60	VMware, Inc.
192.168.73.251	a0:8	4	240	Hewlett Packard
192.168.73.3	00:5	1	60	VMware, Inc.
192.168.1.19	00:5	1	60	VMware, Inc.
192.168.1.19	00:5	1	60	VMware, Inc.
192.168.1.199	00:0	1	60	VMware, Inc.
192.168.1.201	24:b	1	60	Hewlett Packard
192.168.1.202	6c:3	1	60	Hewlett Packard
192.168.1.220	d8:9	1	60	Hewlett Packard
192.168.1.251	00:5	1	60	VMware, Inc.

Passwörter (1)

- Standard Passwörter
  - admin, root, 1234, 0000, pass0rd, vnc, <leer>
- Default Passwörter
  - https://github.com/danielmiessler/SecLists
- Schwache Passwörter
  - Sommer2022
  - Winter2022
  - dieter
  - **1** (Administrator!)
- Data Breaches
  - https://haveibeenpwned.com/

Vendor	Username	Password
2Wire, Inc.	http	<BLANK>
360 Systems	factory	factory
3COM	3comcso	RIP000
3COM	<BLANK>	12345
3COM	<BLANK>	1234admin

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Passwörter (2)

- Active Directory
  - Zugriff ohne Domain Account möglich
  - Passwort im Kommentar Feld
  - Initial Passwörter nicht geändert
- Password Spraying
  - Winter2023!
  - Initial Passwort (welcome, ChangeMe,...)
- Hersteller (Backdoor Account)
  - Download Config File via FTP – root PW im Klartext
  - Download Firmware Image – Crack Password Hash
- VNC Zugang
  - Kein Passwort
  - Numerisches Passwort

Password Spraying Attack

Author: Rishu Ranjan

Description

Password spraying is a type of brute force attack. In this attack, an attacker will brute force logins based on list of usernames with default passwords on the application. For example, an attacker will use one password (say, Secure@123) against many different accounts on the application to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.

This attack can be found commonly where the application or admin sets a default password for the new users.

https://owasp.org/www-community/attacks/Password_Spraying_Attack

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Passwörter (3)

- NBNS, LLMNR, MDNS
  - Fehlende Namensauflösung via DNS
  - Alte Systemnamen
  - wpad
  - Password Hashes von Domain Benutzer
  - 20-30% knackbar innerhalb von 4h
- IPv6 DNS, DHCP
  - IPv6 parallel zu IPv4 aktiv
  - Info Rogue DNS Server verteilen
  - IPv6 wird bevorzugt
- IPMI – Protokoll Schwachstelle
  - Passwort Hash auslesen
  - Passwort Cracking
  - Default Passwort – 8 Stellen Alphanumerisch

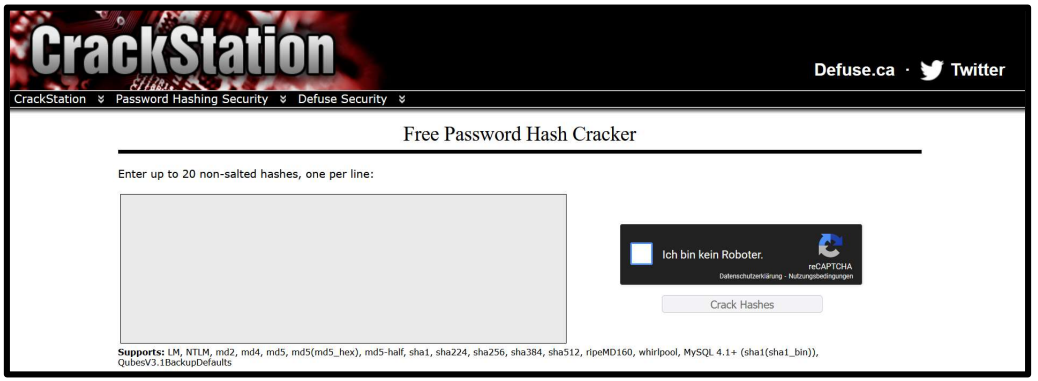
Privilege escalation, lateral movement

- Lokale Adminrechte von Domain Benutzern
  - Zugriff auf lokale SAM DB
  - Lokalen Administrator Hash auslesen

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:edfc4c90d11bc45fae0aa785e3f27d55:::
```

  - Password Crack
  - Password Rainbow Table

- Lokaler Admin Account
  - Passwort ident auf vielen Systemen
  - PTH – Pass the hash



https://crackstation.net/

Sensitive Informationen

- Drucker / Scanner
  - Keine Zugriffsbeschränkung
  - Gescannte, vertrauliche Dokumente
- SMB Shares
  - Schreibbar für alle User
  - Konfigurationsdateien von Cisco Geräten
  - Konfigurationsdateien von Anwendungen
  - WinSCP Konfig Datei
  - Backup eines Komplettsystems
- Unsichere Protokolle
  - FTP, TELNET, MODBUS

```
security passwords min-length 8
no logging console
enable secret 5 $1$p8Y6$MCdRLBzuGlfOs9S.hXOp0.
!
username hub password 7 02501705B3907344E
username admin privilege 15 password 7 10181A325528130F010D24
username guest password 7 124F163C42340B112F3830
```

https://www.ifm.net.nz/cookbooks/passwordcracker.html

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Zusammenfassung

- Fehlende Netzwerk Segmentierung
- Weg ins Internet möglich
- Passwörter!
- Veraltete Systeme / Updates
- Unsichere Protokolle
- Fehlendes Verständnis IT vs. OT
- Fehlendes Security KnowHow
- Zusammenarbeit IT und OT

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Vielen Dank!