HanseSecure

Exploit Hunter

Der Letzte macht die Tür zu

Unverschlossene Büros als Einladung für Hacker

vom 19.09.2020

Inhaltsverzeichnis

1. Wer

Wer

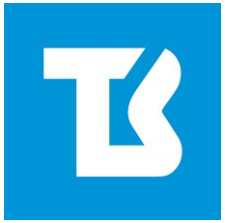
- 21 CYBERSECURITY TWITTER ACCOUNTS YOU SHOULD BE FOLLOWING

  (https://www.sentinelone.com/blog/21-cybersecurity-twitter-accounts-you-should-follow/)

“Florian is a redteamer, pentester and exploit hunter, as well prolific tweeter and blogger. @HanseSecure is one of the best sources for tweets and retweets of technical write-ups, links to scripts, plug-ins, exploit kits and other new tools, along with how-to’s and tips for anyone interested in redteaming and pentesting.”

- Modern red teaming: 21 resources for your security team

  (https://techbeacon.com/security/modern-red-teaming-21-resources-your-security-team)



“Hansemann is an ethical hacker and penetration tester. His tweets and blog focus on tools and techniques of interest to red team members. For example, he covers Tokenvator—a tool to elevate privilege with Windows tokens—and how to write a payload for process injection in Windows.”

Wer

- Disclosure CVE-2020-13912
  (https://hansesecure.de/2020/06/vulnerability-in-monitoring-software/?lang=en)

- Microsoft SmartScreen Bypass
  (https://hansesecure.de/2019/05/smartscreen-bypass/)

- Disclosure CVE-2018-7272
  OpenAM Unauthorized Access
  (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7272)

- Disclosure CVE-2018-16231
  Remote DoS in Personal FTP-Server
  (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16231)

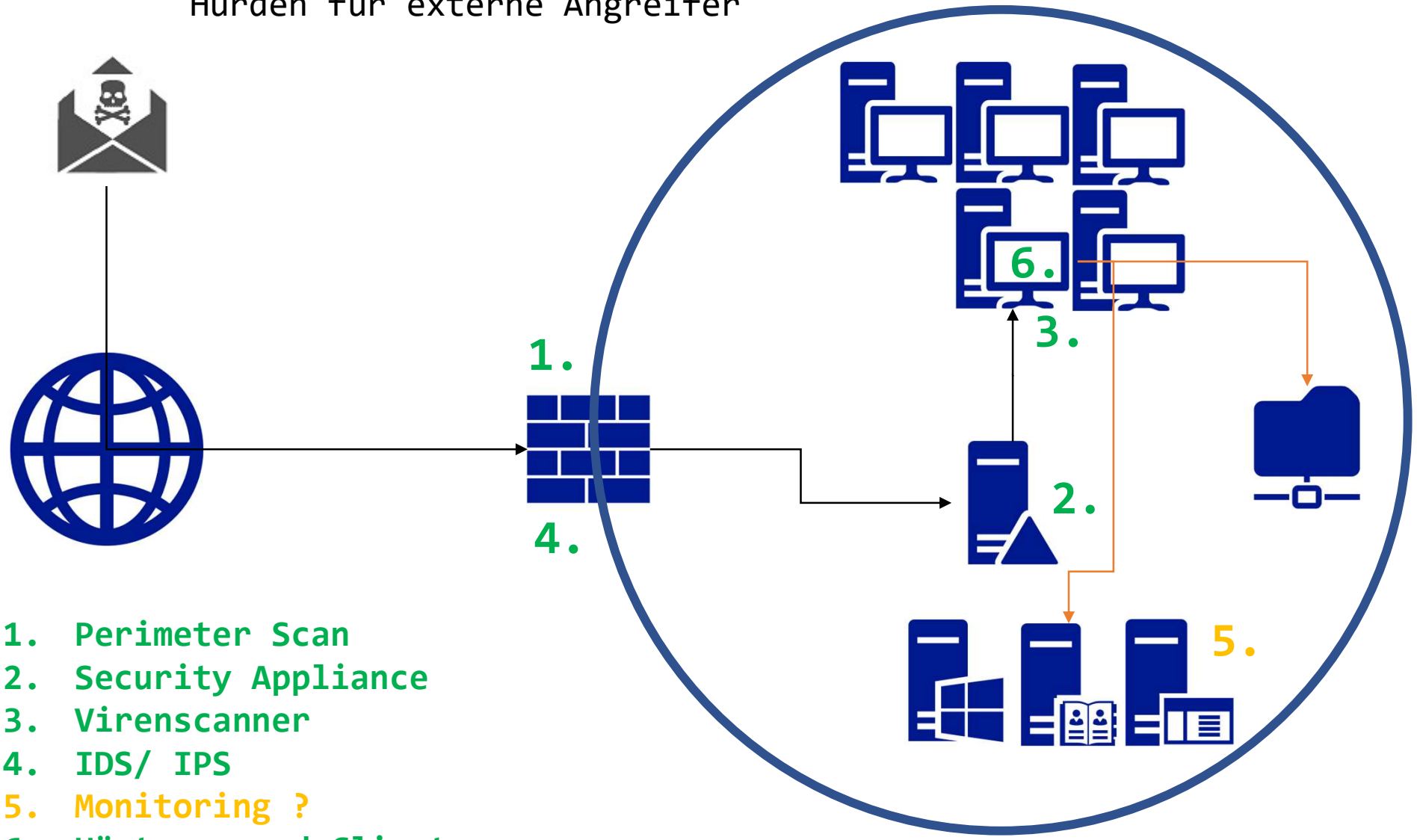
- Intel Vulnerability
  (https://hansesecure.de/2019/05/intel-unquoted-service-path/)

- Artikel: IT-Sicherheit professionell unter die Lupe nehmen
  (https://www.security-insider.de/it-sicherheit-professionell-unter-die-lupe-nehmen-a-852288/)

2. Warum

Warum

Hürden für externe Angreifer

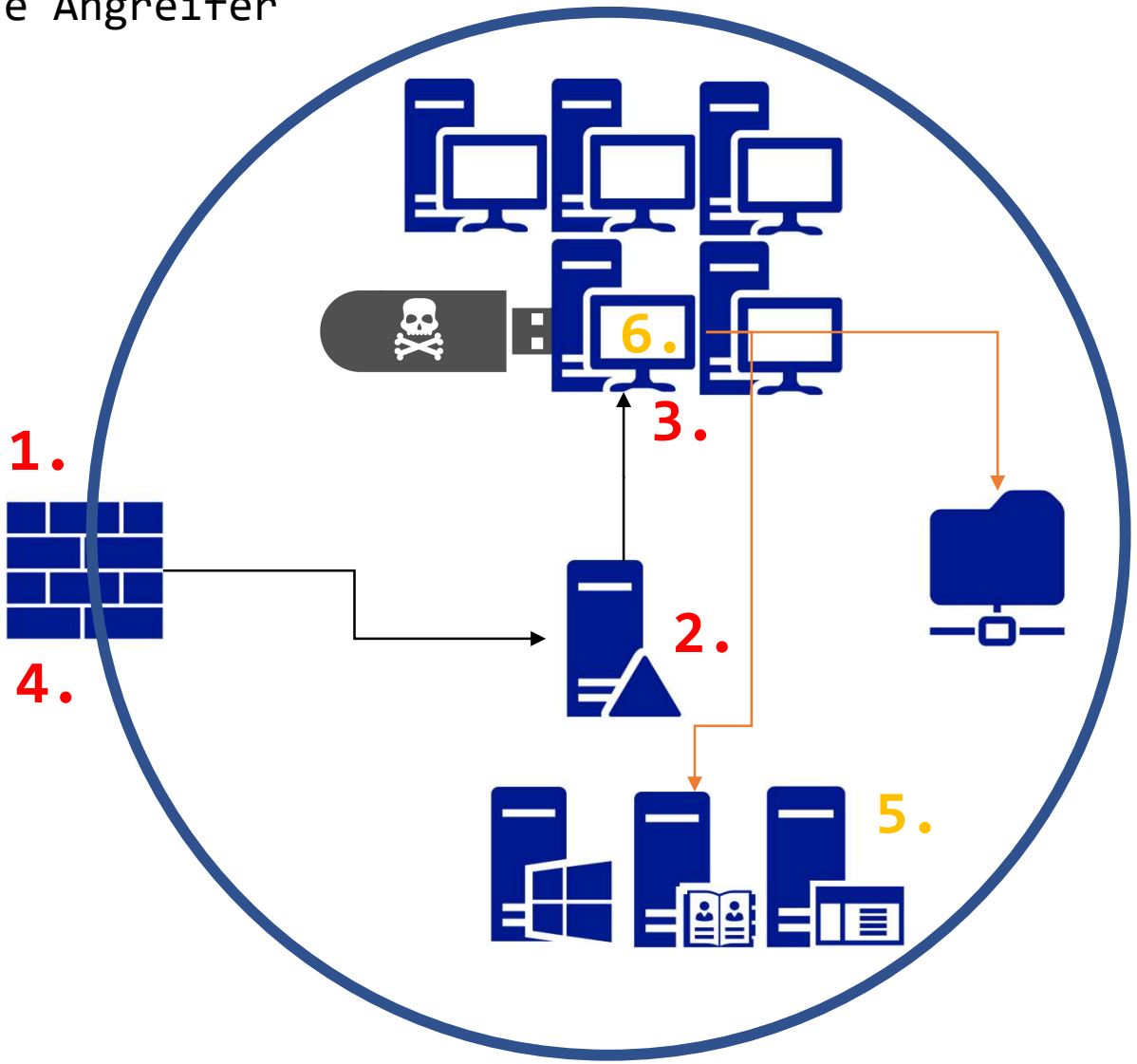


1. Perimeter Scan
2. Security Appliance
3. Virenscanner
4. IDS/ IPS
5. Monitoring ?
6. Härtungsgrad Client

@CyberWarship

Warum

Hürden für interne Angreifer



1. ~~Perimeter Scan~~
2. ~~Security Appliance~~
3. ~~Virenscanner~~
4. ~~IDS/ IPS~~
5. Monitoring ?
6. Härtungsgrad Client

@CyberWarship

Warum

3. Wie

Wie

Wie

Keine Verschlüsselung ohne BIOS-Passwort

Szenario

1. Unverschlossene Tür, 15 Minuten unbeaufsichtigt
2. Eigenes Live OS booten
3. Systemlevel-Backdoor einrichten
4. HelpDesk ein „Problem“ via RDP lösen lassen
5. Mimikatz
6. Profit

Potentielles Risiko

9

Wie

I. Keine Verschlüsselung ohne BIOS-Passwort

1. Bootreihenfolge ändern
2. Von Live Medium booten (OS Egal, z.B. Linux)
3. sethc.exe gegen cmd.exe tauschen

   copy C:\Windows\System32\sethc.exe C:\Windows\System32\sethc.exe.bak
   copy C:\Windows\System32\cmd.exe C:\Windows\System32\sethc.exe
4. Bootreihenfolge wiederherstellen
5. Einrastfunktion bei Login auslösen (5x Shift)
6. Neuen Local Admin hinzufügen

   net user HanseSecure SuperSexy123! /add
   net localgroup Administratoren HanseSecure /add

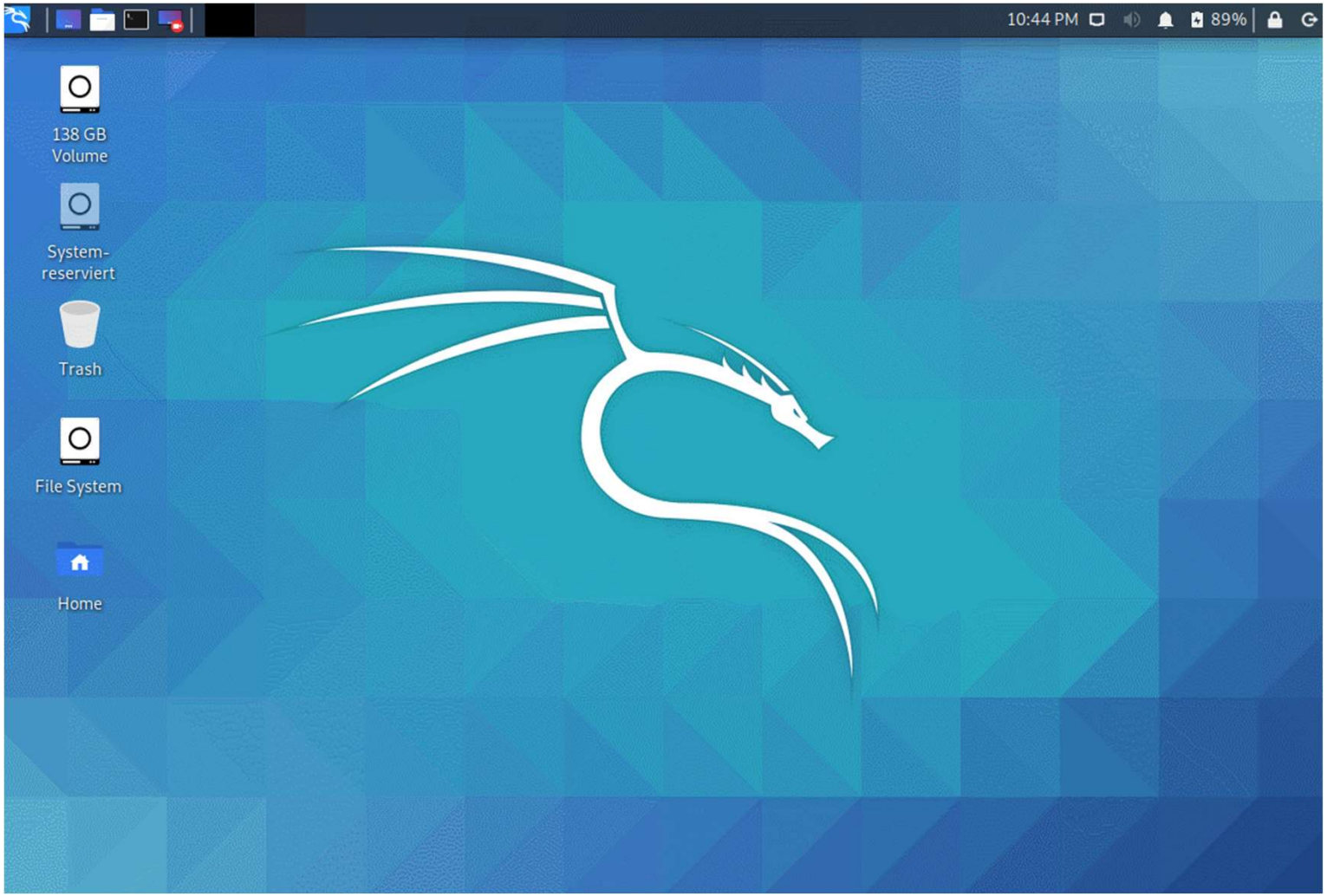
Wie

I. Keine Verschlüsselung ohne BIOS-Passwort

DEMO

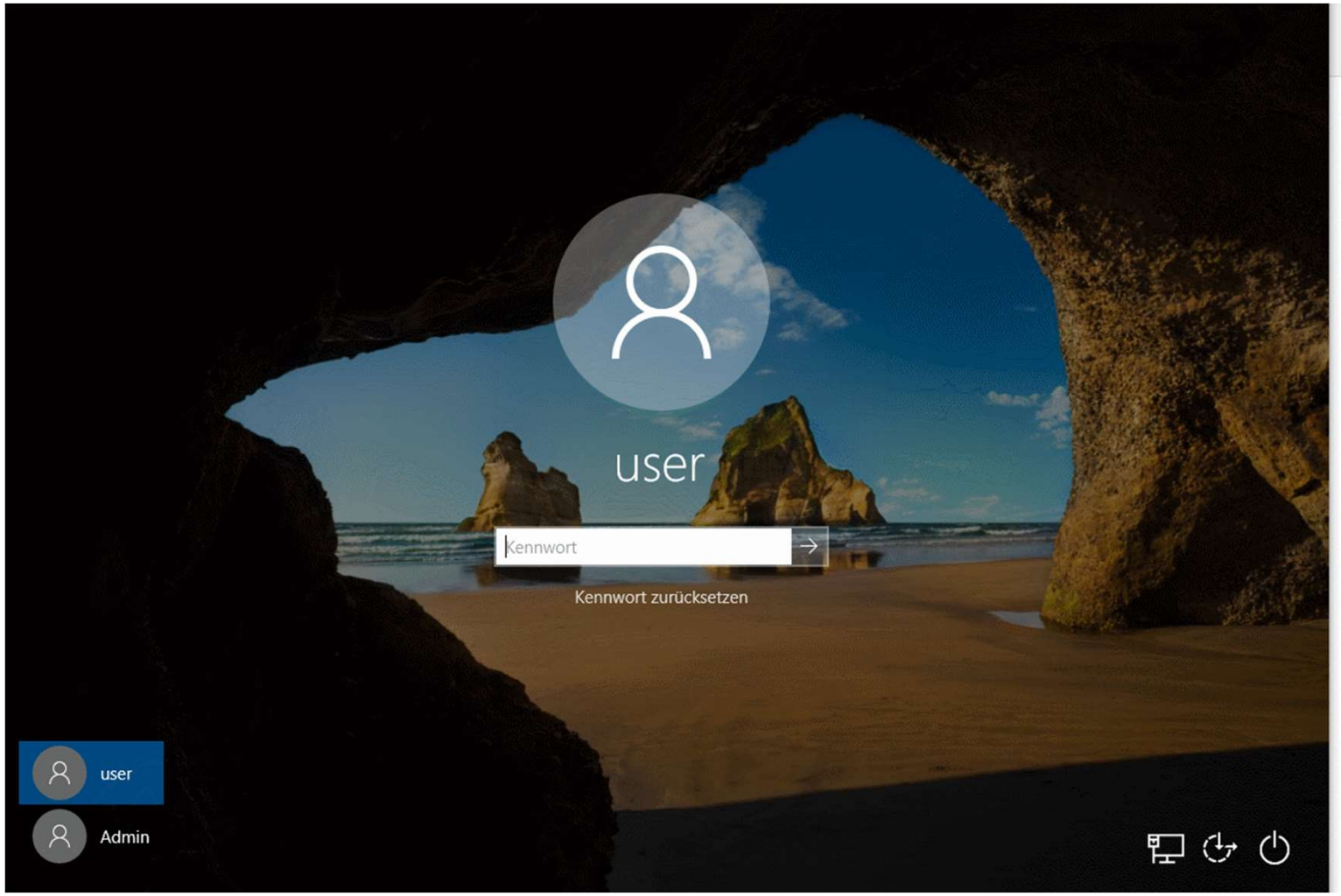
Wie

I. Keine Verschlüsselung ohne BIOS-Passwort



Wie

I. Keine Verschlüsselung ohne BIOS-Passwort



Wie

I. Keine Verschlüsselung ohne BIOS-Passwort

Wie

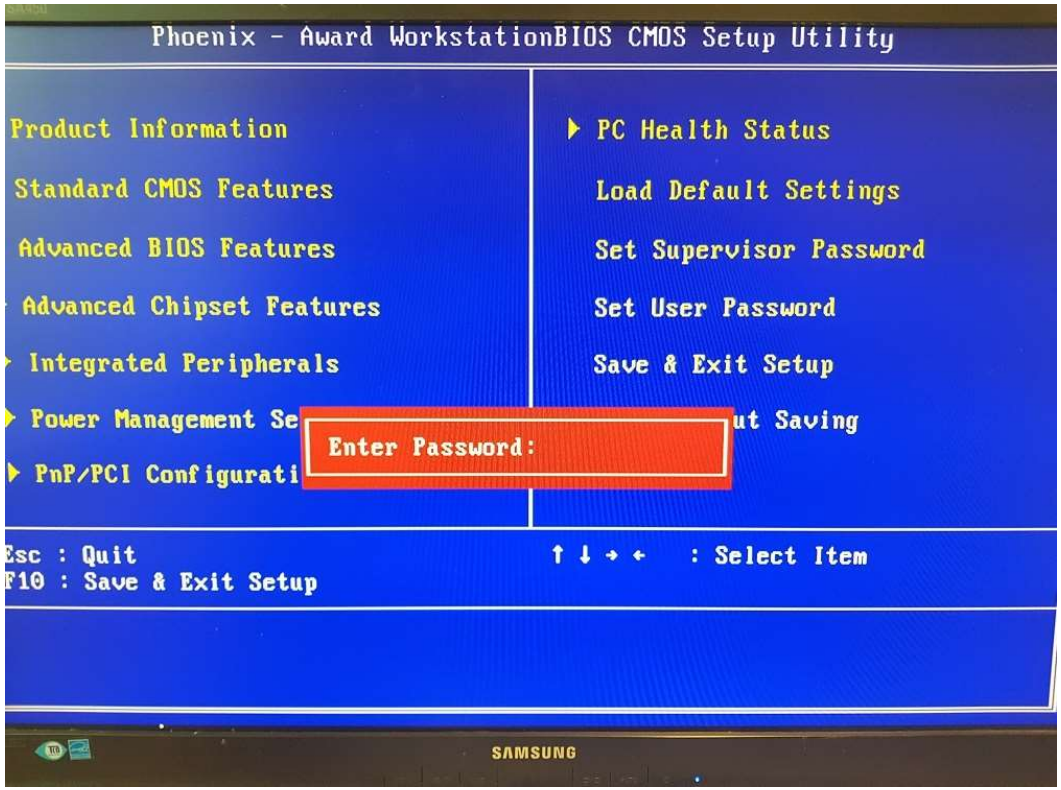
II. Keine Verschlüsselung mit BIOS-Passwort

Szenario

1. Unverschlossene Tür, 60 Minuten unbeaufsichtigt
2. BIOS-Passwort Bypass
3. Eigenes Live OS booten
4. Backdoor einrichten
5. Neuen Admin Anlegen
6. HelpDesk ein „Problem“ via RDP lösen lassen
7. Mimikatz
8. Profit

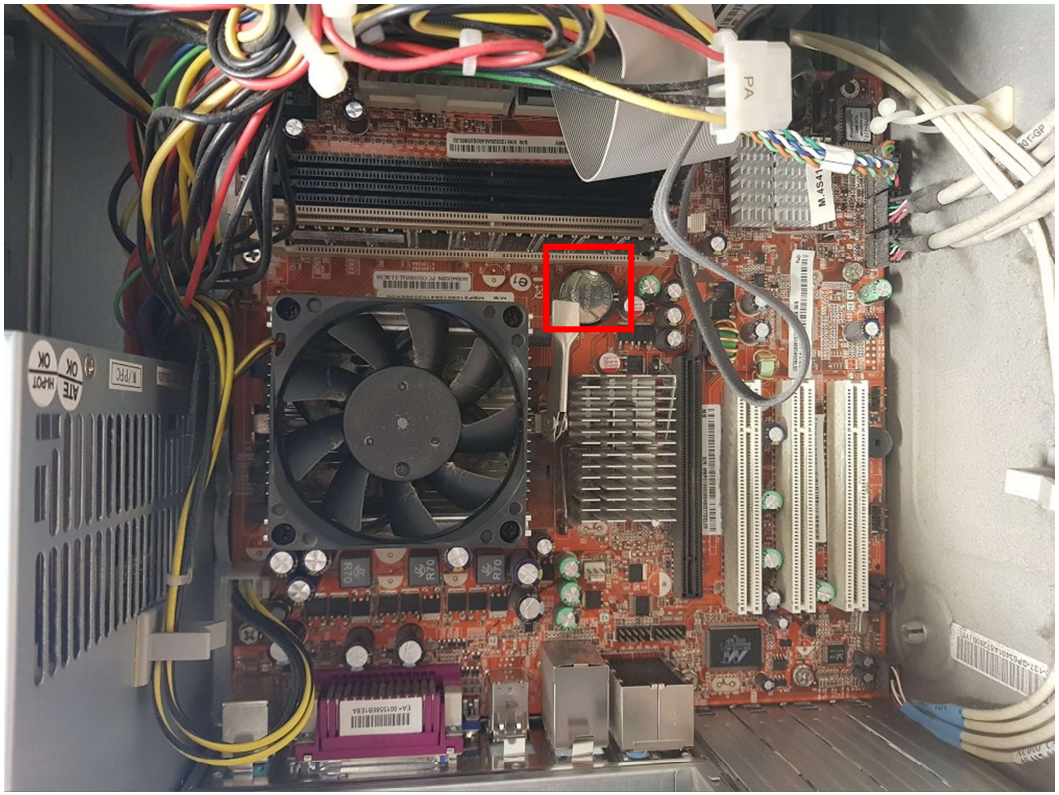
Potentielles Risiko

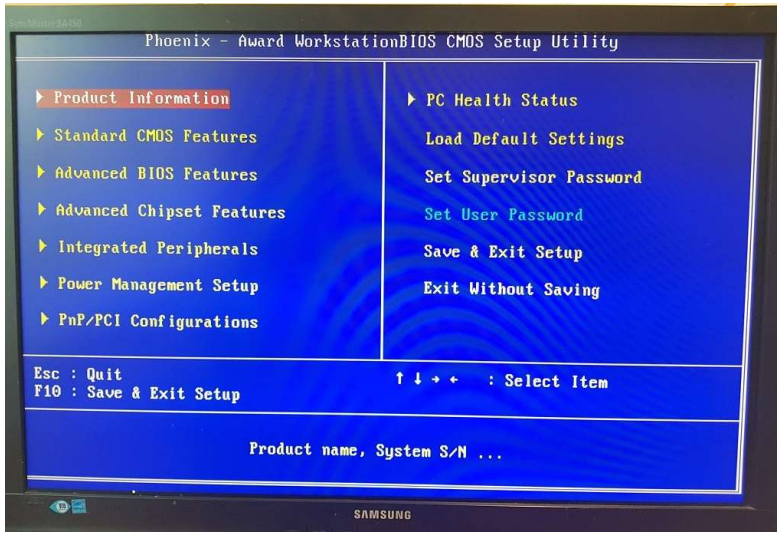
8



Wie

II. Keine Verschlüsselung mit BIOS-Passwort





Wie

II. Keine Verschlüsselung mit BIOS-Passwort

Desktop Computer

1. Jumper/ CMOS Batterie entfernen
2. Neustart ohne BIOS Pw ;-)
3. Schritte aus I.)

Laptop

1A. Jumper/ CMOS Batterie entfernen
2A. Neustart ohne BIOS Pw ;-)
3A. Schritte aus I.)
1B. https://bios-pw.org/
2B. Neustart mit WerksBIOS Pw ;-)
3B. Schritte aus I.)

Wie

II. Keine Verschlüsselung mit BIOS-Passwort

BIOS Password Recovery for Laptops

Quick and easy way to recover BIOS passwords on laptops. Based on research by Dogbert and Asyncritus.

Enter your code

Code

Get password

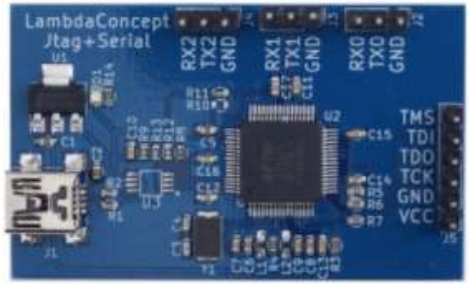
https://bios-pw.org/

Wie

III. Festplattenverschüsselung (Bitlocker) ohne Preboot

Szenario

1. Unverschlossene Tür, 180 Minuten unbeaufsichtigt
2. Bitlocker Bypass
3. Backdoor einrichten
4. Neuen Admin Anlegen
5. HelpDesk ein „Problem“ via RDP lösen lassen
6. Mimikatz
7. Profit



Potentielles Risiko

7

Wie

III. Festplattenverschüsselung (Bitlocker) ohne Preboot

August 26, 2020, 5:57 pm
Arrived Shipping Partner Facility, USPS Awaiting Item
BELL GARDENS, CA 90201
Shipping Partner: APC Postal Logistics

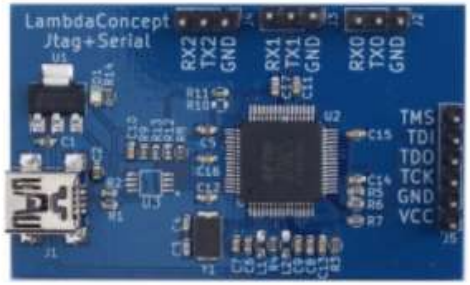
Thank you, order received! Aug 26
USA 06:46

Shipping via Passport with love

IV. Festplattenverschüsselung (Bitlocker) mit weak Preboot

Szenario

1. Unverschlossene Tür, 180 Minuten unbeaufsichtigt
2. PIN raten (1234? ;-)
3. Bitlocker Bypass
4. Backdoor einrichten
5. Neuen Admin Anlegen
6. HelpDesk ein „Problem“ via RDP lösen lassen
7. Mimikatz
8. Profit



Potentielles Risiko

6

Wie

V. Keylogger (physisch)

Szenario

1. Unverschlossene Tür, 5 Minuten unbeaufsichtigt
2. Keylogger zwischen Tatstatur und Computer anschließen
3. Stick bei nächsten Gelegenheit mitnehmen oder Premium mit Wifi ;-)
4. Profit

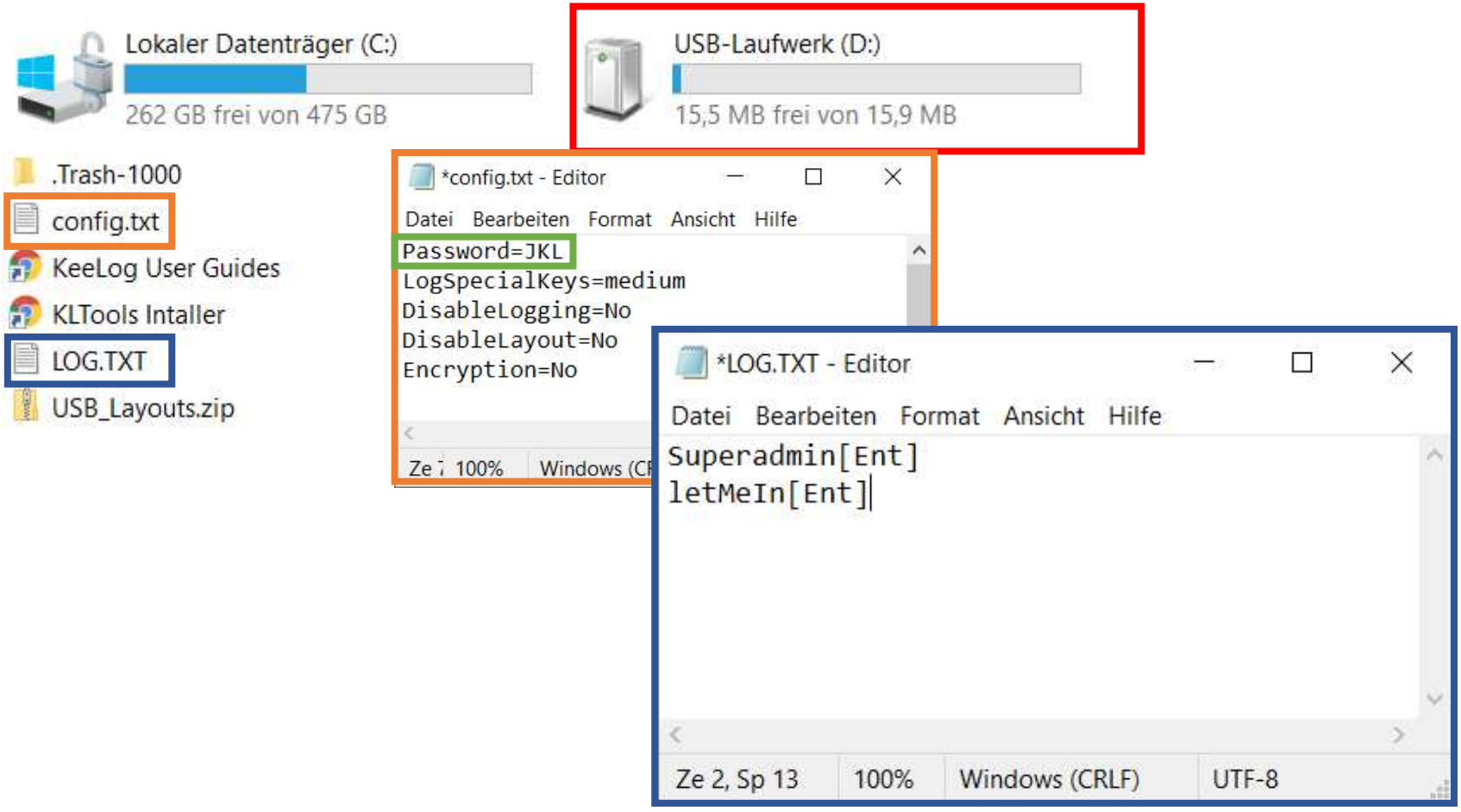
Potentielles Risiko

4

Wie

V. Keylogger (physisch)

„Geheime“ Tastenkombi drücken -> Wechsel in Datenträger



Wie

VI. Rubber Ducky

Szenario

1. Unverschlossene Tür, ungesperrtes System,
   5 Minuten unbeaufsichtigt
2. Rubber Ducky an beliebigen USB-Port
3. Profit

Potentielles Risiko

7

Wie

VI. Rubber Ducky

Payload-Vorlagen

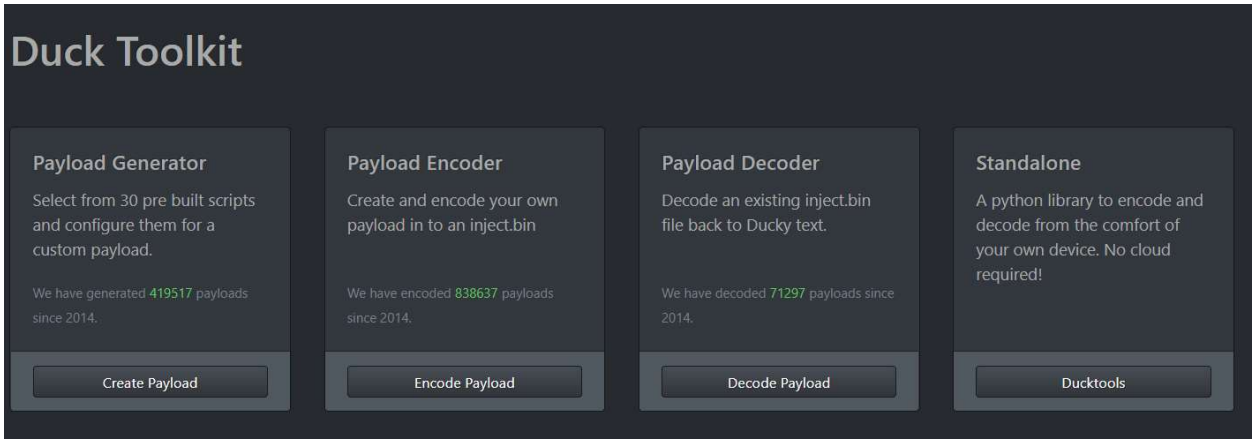
https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads

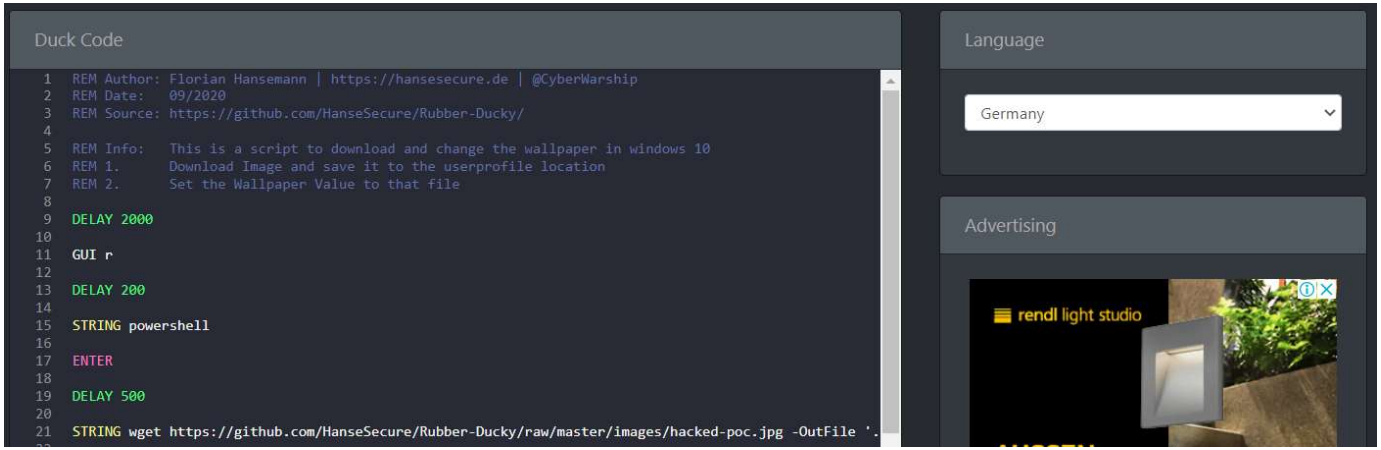
- Payload - Non-Malicious Auto Defacer
- Payload - Open Webpage, Any Platform
- Payload - Lock Your Computer Message
- Payload - Ducky Downloader
- Payload - Ducky Phisher
- Payload - FTP Download / Upload
- Payload - Restart Prank
- Payload - Silly Mouse, Windows is for Kids
- Payload - Windows Screen rotation hack
- Payload - Powershell Wget + Execute
- Payload - mimikatz payload
- Payload - MobileTabs
- Payload - Create Wireless Network Association (AUTO CONNECT) PINEAPPLE
- Payload - Retrieve SAM and SYSTEM from a live file system
- Payload - Ugly Rolled Prank
- Payload - XMAS
- Payload - Pineapple Assocation (VERY FAST)
- Payload - WiFun v1.1
- Payload - MissDirection
- Payload - Remotely Possible
- Payload - Batch Wiper/Drive Eraser
- Payload - Copy File to Desktop
- Payload - Youtube Roll
- Payload - Disable AVG 2012
- Payload - Disable AVG 2013
- Payload - EICAR AV test
- Payload - Download mimikatz, grab passwords and email them via gmail
- Payload - Hotdog Wallpaper
- Payload - Android 5.x Lockscreen
- Payload - Chrome Password Stealer
- Payload - Website Lock
- Payload - Windows 10 : Download & Change Wallpaper
- Payload - Windows 10 : Download & Change Wallpaper another version
- Payload - Windows 10 : Download and execute file with Powershell
- Payload - Windows 10 : Disable windows defender
- Payload - Windows 10 : Disable Windows Defender through powershell
- Payload - Windows 10 : Wifi, Chrome Dump & email results
- Payload - Windows 7 : Logoff Prank
- Payload - Netcat Reverse Shell
- Payload - Fake Update screen
- Payload - Rickroll
- Payload - Fast Meterpreter
- Payload - Data-Exfiltration / Backdoor

Wie

VI. Rubber Ducky

Payload selbst erstellen
https://ducktoolkit.com/





VI. Rubber Ducky

DEMO

Wie

VII. BashBunny

Szenario

1. Unverschlossene Tür, ungesperrtes System,
   5 Minuten unbeaufsichtigt
2. BashBunny an beliebgen USB-Port
3. Profit

Potentielles Risiko

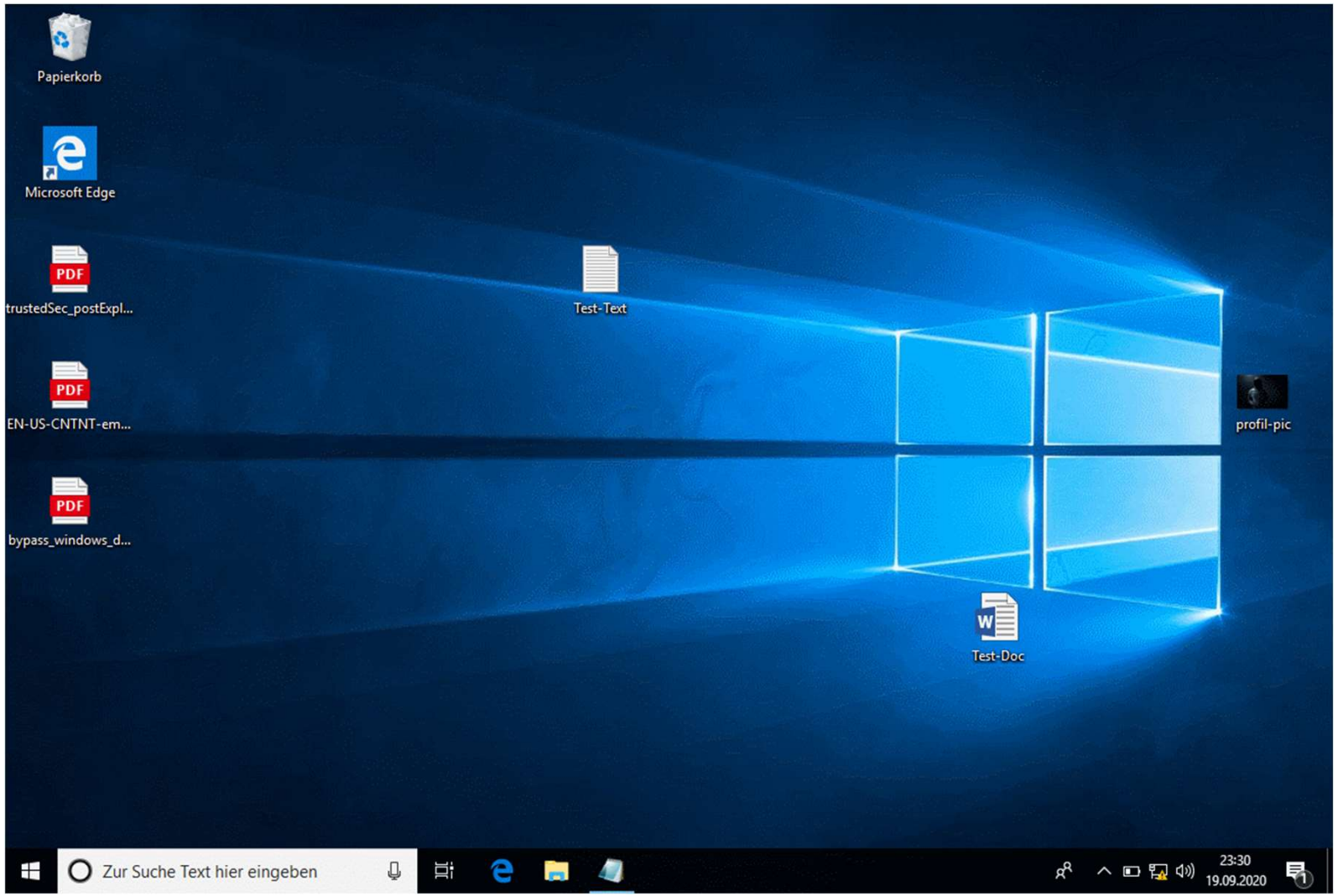
7

VII. BashBunny

DEMO

Wie

VII. BashBunny



Wie

VIII. LAN Turtle

Szenario

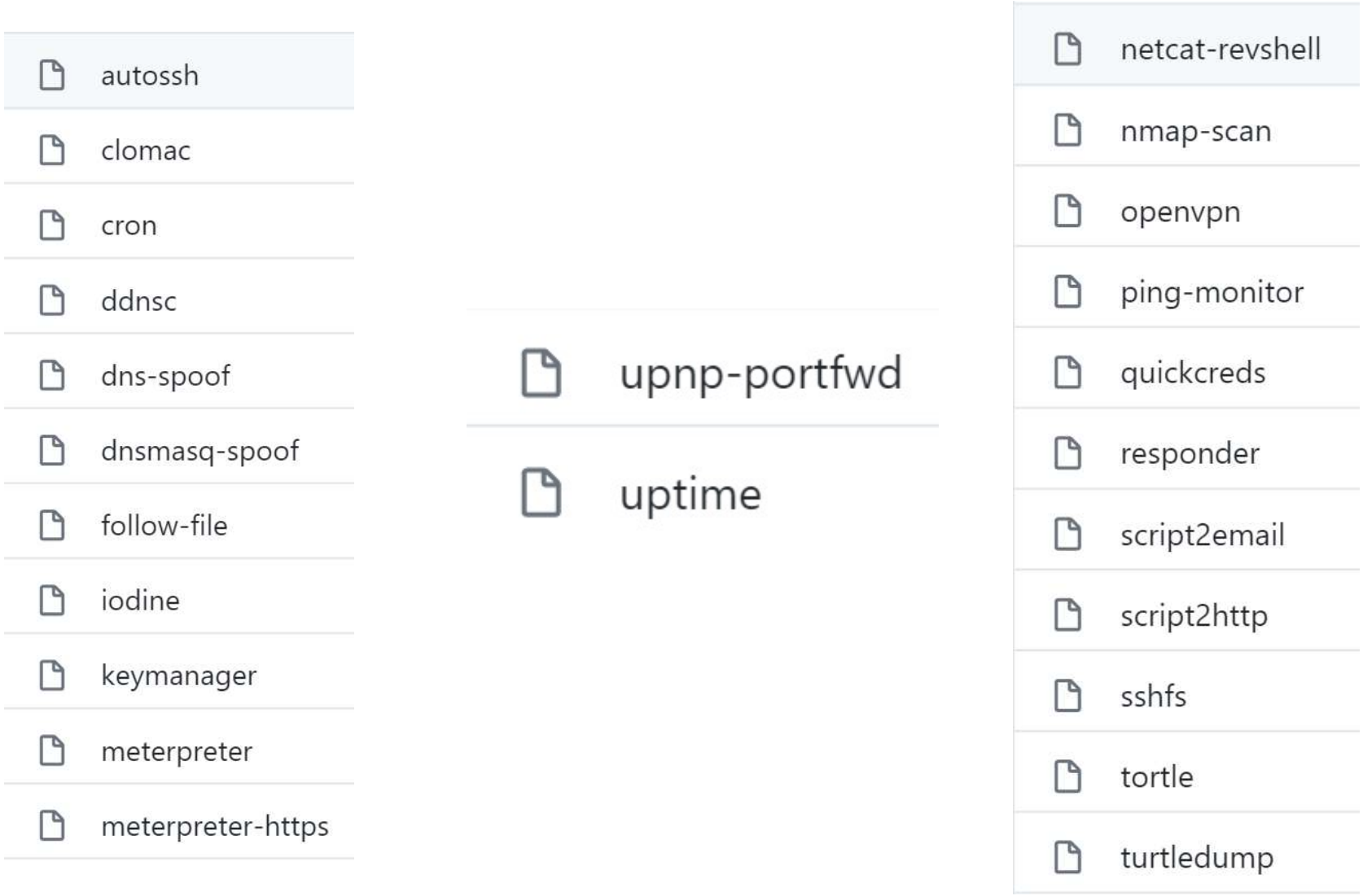
1. Unverschlossene Tür, ungesperrtes System,
   2 Minuten unbeaufsichtigt
2. LAN Turtle zwischen eingehenden LAN und einem USB Port anschließen
3. Profit

Potentielles Risiko

7

Wie

VIII. LAN Turtle



VIII. LAN Turtle

DEMO

Wie

IX. SharkJack

Szenario

1. Unbeaufsichtigte & aktivierte LAN-Dose,
   2 Minuten unbeaufsichtigt
2. SharJack an LAN anschließen, Angriff abwarten, Abziehen
3. Profit

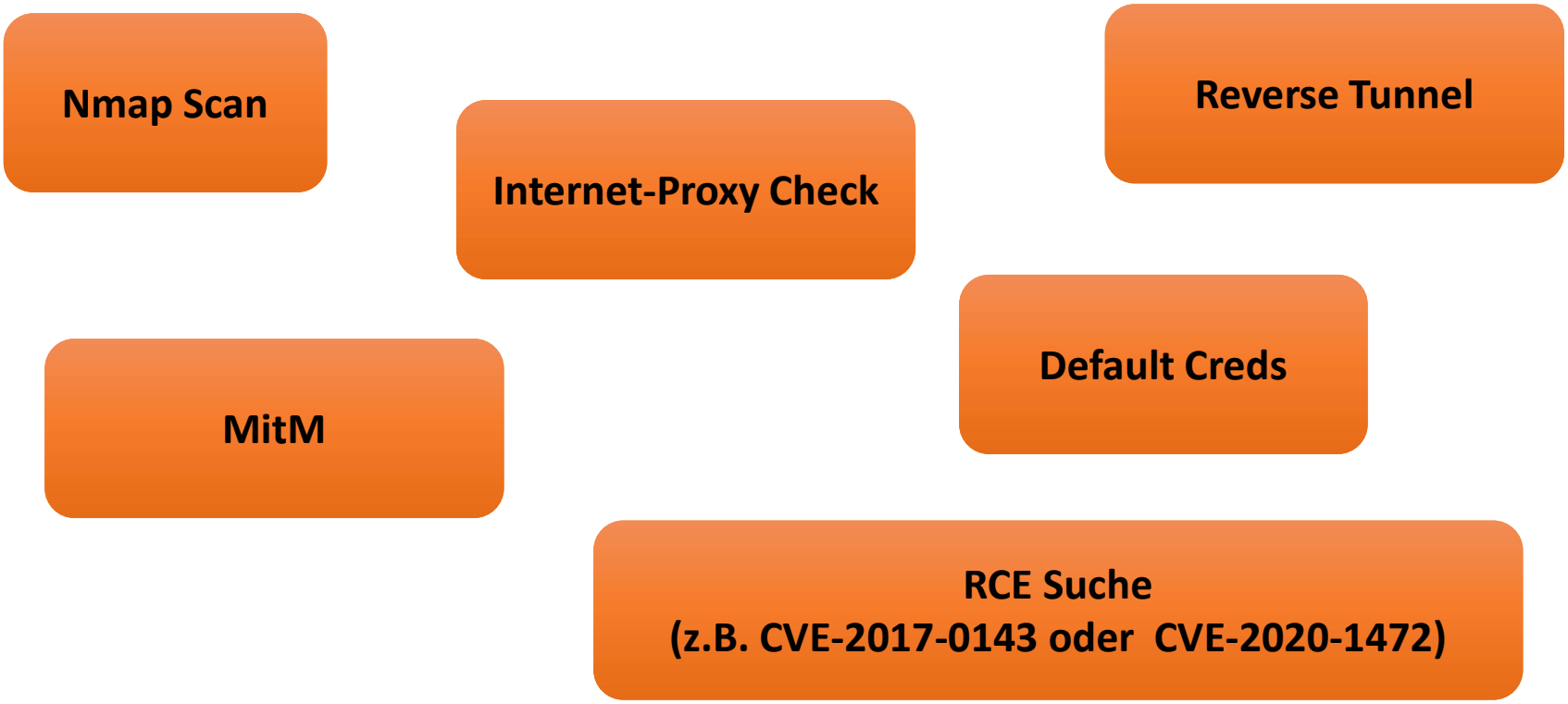
Potentielles Risiko

7

Wie

IX. SharkJack

Der SharkJack besitzt ein vollfunktionsfähiges Linux Betriebssystem, welches beliebige vorkonfigurierte Befehle automatisch ausführt, sobald dieser eine Netzwerkverbindung herstellen kann.



DEMO

Wie

X. Raspberry Pi

Szenario

1. Unverschlossene Tür, offener & aktiver Netzwerkanschluss, 15 Minuten unbeaufsichtigt
2. RaspBerry an Netzwerkdose
3. Automatischer Reverse SSH oder VPN Tunnel
4. Profit

Potentielles Risiko

7

Wie

XI. Statisches NAC

Szenario

1. Unverschlossene Tür, offener & aktiver Netzwerkanschluss, 30 Minuten unbeaufsichtigt
2. MAC von Laptop oder Drucker notieren
3. Eigene MAC Adresse anpassen
4. SMB Signing? -> SMB Relay
5. Profit

Potentielles Risiko

7

Wie

XI. Statisches NAC

Window

```
Set-NetAdapter -Name "Ethernet 1"
-MacAddress "00-10-18-57-1B-0D"
```

Linux

```
sudo ifconfig en0 ether
00-10-18-57-1B-0D
```

4. Fazit

Fazit

1. Computer immer Sperren
2. Räume mit Netzwerkanschlüssen oder IT-Systemen nicht länger als 15 Minuten unverschlossen lassen.
3. Großraum PC herunterfahren

HanseSecure

Exploit Hunter

Danke für Eure Zeit!

Florian Hansemann

Principal Security Consulntant

Web hansesecure.de
Mail info@hansesecure.de
Twitter @CyberWarship