PENETRATIONSTESTS

EIN TAG IM LEBEN EINES PENETRATIONSTESTERS – IN 45MIN

Gastvortrag von Christian Stehle

26.06.2023

EINLEITUNG - WHOAMI

- Saß auch mal da vorne
- Senior Pentester / Lead "Adversary Emulation" @ it.sec (2017 – 2023)
  - Penetrationstests & Red Teaming A-Z
- Ab Oktober eigene Firma
- Inhaltlich spezialisiert auf Infrastruktur / Active Directory
- Sammle gern Zertifizierungen (OSCP, OSEP, OSWE, CRTO, CRTP, eCTPX, "Red Team Lead")

DAS WICHTIGSTE VORAB...

- Abkürzung ist Pentest

  Nicht PEN Test (Kein Akronym, wir testen auch keine Stifte!)

EINLEITUNG – WARUM PENTESTS

- Cyberkriminalität nimmt zu – bin ich / mein Unternehmen der Nächste?
- In Deutschland:
  - Ausgaben für IT-Sicherheit: ca. 6,9 Mrd. € (2021) (Quelle)
  - Prognose: steigt weiter
  - Schaden: ca. 203 Mrd. € (2021) (Quelle)

EINLEITUNG – WARUM PENTESTS

- Wie beantwortet man die Frage, ob ich "der Nächste" bin?
- Mit einem Penetrationstest werden Schwachstellen identifiziert
- Durch Ausnutzen einer Schwachstelle wird ein Sicherheitsziel (Teaser: Klassisch vs. Mehrseitig) verletzt
- Wenn man die Schwachstellen kennt, kann man Gegenmaßnahmen einleiten (oder sich entscheiden, das Risiko zu tragen)

EINLEITUNG - AGENDA

- GRUNDLAGEN
- IM TEST
  - RECON
  - METASPLOIT
  - BURPSUITE
- NACH DEM TEST

GRUNDLAGEN – WAS IST EIN PENTEST? BESCHREIBUNG (BSI)

- Siehe Abschnitt "1.3 Begriffsbestimmung IS-Penetrationstest":
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST?

- Ziel eines Pentests: Schwachstellen identifizieren/aufdecken
- Durch einen Pentest kann ein System(-verbund) sicherheitstechnisch bewertet werden
- Ein Penetrationstest selbst behebt keine Schwachstellen
- Prüfer setzt Methoden wie echte Angreifer ein, um Schwachstellen zu finden und zu verifizieren
- Prüfobjekte können sehr vielfältig sein, solange ihr Angreifer-Denke habt und Schwachstellen sucht - und dafür beauftragt wurdet - würde ich es als Pentest bezeichnen ☺

  (Web-)Anwendungen

  Infrastruktur

  Hardware-Komponenten

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST? SCHWACHSTELLEN

- Schwachstelle ist eine Verwundbarkeit, die ein Sicherheitsrisiko darstellt
- Eine Schwachstelle kann ausgenutzt werden, um ein Sicherheits-Ziel zu verletzen
  - Zumindest in der Theorie. In der Praxis gibt es weniger schwarz/weiß und beim Ausnutzen spielen andere Faktoren eine Rolle, wodurch das tatsächliche Ausnutzen dann doch nicht klappt. Auch unser Job: rausfinden ob was tatsächlich ausgenutzt werden kann
- Beispiele:
  - Authorization Bypass = ich brauch keine gültigen Zugangsdaten
  - SQL Injection = ich kann auf die ganze Datenbank zugreifen
  - Buffer Overflow = ich kann den Programmfluss kontrollieren und eigene Befehle ausführen
  - Default Password = ich kann die Logindaten im Hersteller-Handbuch nachlesen

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST? VORGEHENSWEISEN

- Black Box

  Keine Informationen über Zielsysteme, keine Zugänge

  Eingeschränkte Sicht

- White Box

  Informationen vorhanden, Zugänge vorhanden, Quellcode vorhanden

  Hohe Abdeckung

- Gray Box

  Zwischending, z.B. nur normale User und keine administrativen

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST? VORGEHENSWEISEN - STANDARDS

- Standards beschreiben das Vorgehen, einzelne Prüfpunkte und beinhalten Checklisten, z.B.

  OWASP Web Security Testing Guide

  OWASP Mobile Application Security Testing Guide

  BSI - Durchführungskonzept für Penetrationstests

- Dennoch: ein Pentest kann nicht durch einen Flowchart o. Ä. abgebildet werden
- Im Test ergeben sich zig Möglichkeiten, einzelne Punkte genauer zu untersuchen – Zeit ist aber begrenzt
- Mit der Zeit entwickelt man ein "Gespür" für die brüchigen Stellen und findet sie

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST?
PRÜFOBJEKTE - WAS TESTET MAN EIGENTLICH?

- (Web)-Anwendungen

  z.B. Online-Banking, Webshop, Bewerberportal, Dokumentensystem,…

- Infrastruktur

  Externe Infrastruktur

  - Alles, was aus dem Internet erreichbar ist, z.B. Webserver, VPN-Gateway, Mailserver,..

  Interne Infrastruktur

  - Ausgangspunkt ist innerhalb der Firma, z.B. ausgehend vom Mitarbeiter-PC

- Protokolle
- Hardware

GRUNDLAGEN – WAS IST EIN PENETRATIONSTEST? ABLAUFPLAN (BSI)

- Siehe Abschnitt "6.3 Vorgehensweise"
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3

IM TEST
DER TEST-TAG BEGINNT

- Als erstes erfolgt die Informationsgewinnung („Reconnaissance“, „Recon“)
- Hier werden so viele Informationen wie möglich gesammelt
- Durch Fingerprinting werden Dienste und ggf. ihre eingesetzte Version/Konfiguration identifiziert
- Auch: sich mit der Anwendung / System vertraut machen

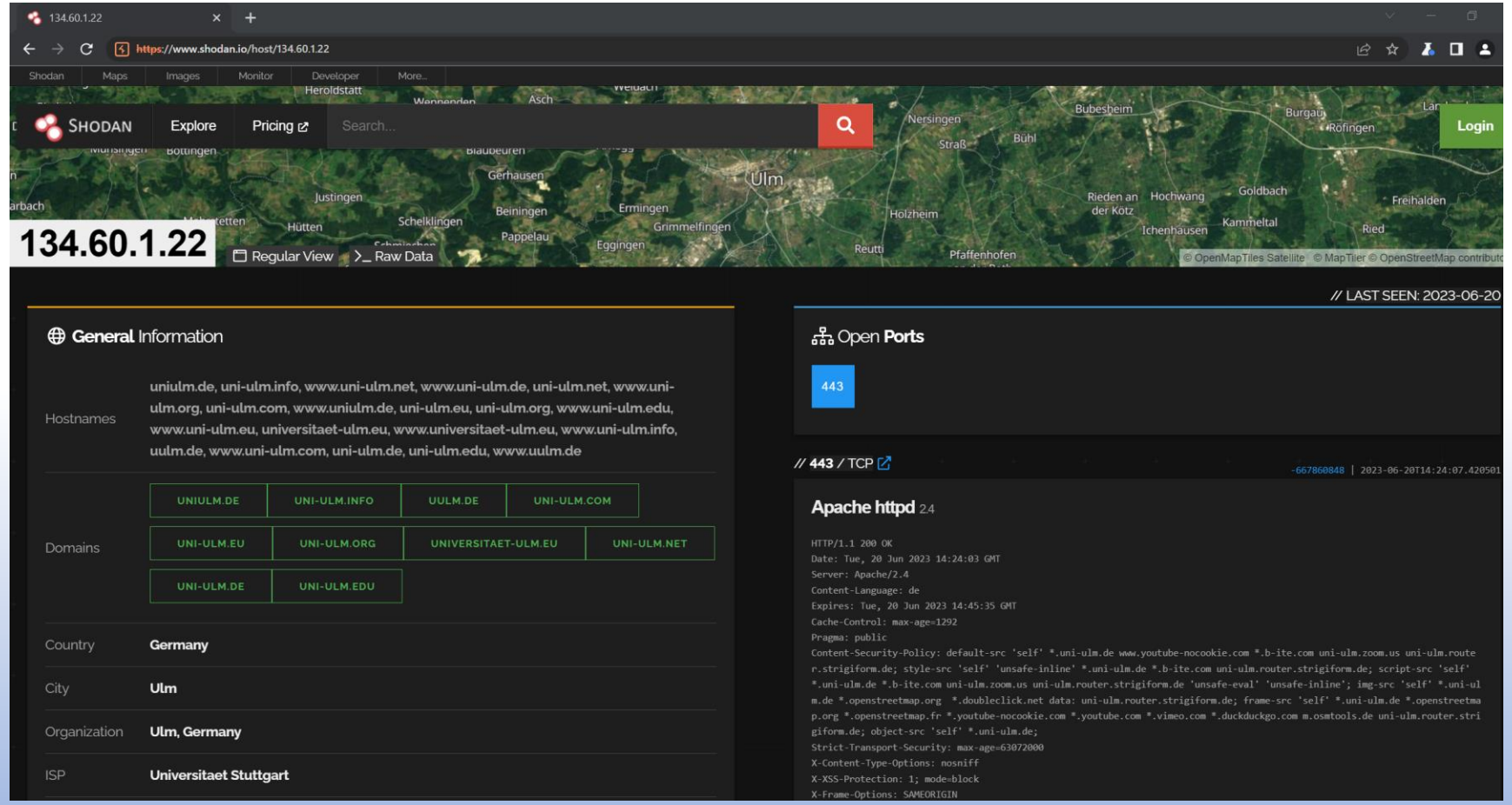
  Was sind die Zwecke, die es erfüllen soll?
- Um Fehler in Konzepten zu finden, muss verstanden werden, was das System tut und wie

IM TEST
RECON: SHODAN

```
rooti@DESKTOP-0GLDJ1G:~$ dig A uni-ulm.de

; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> A uni-ulm.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40435
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;uni-ulm.de.                    IN      A

;; ANSWER SECTION:
uni-ulm.de.             21600   IN      A       134.60.1.22
```

IM TEST

RECON: SHODAN



IM TEST

RECON: NMAP

```
┌──[root@htb-u9bgr7uvhv]─[/home/htb-oxeeql]
└─── #nmap 10.10.10.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 16:53 BST
Nmap scan report for 10.10.10.40
Host is up (0.11s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
```

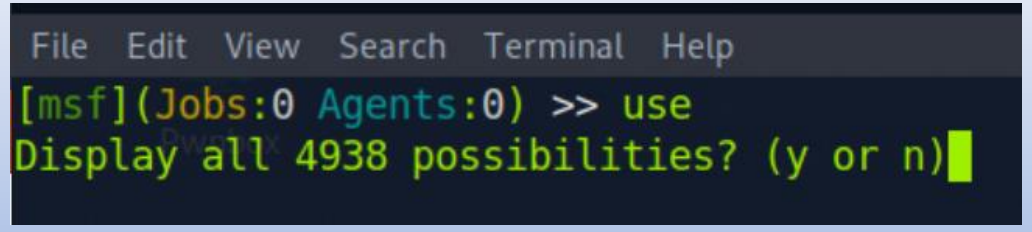
IM TEST

RECON: NMAP

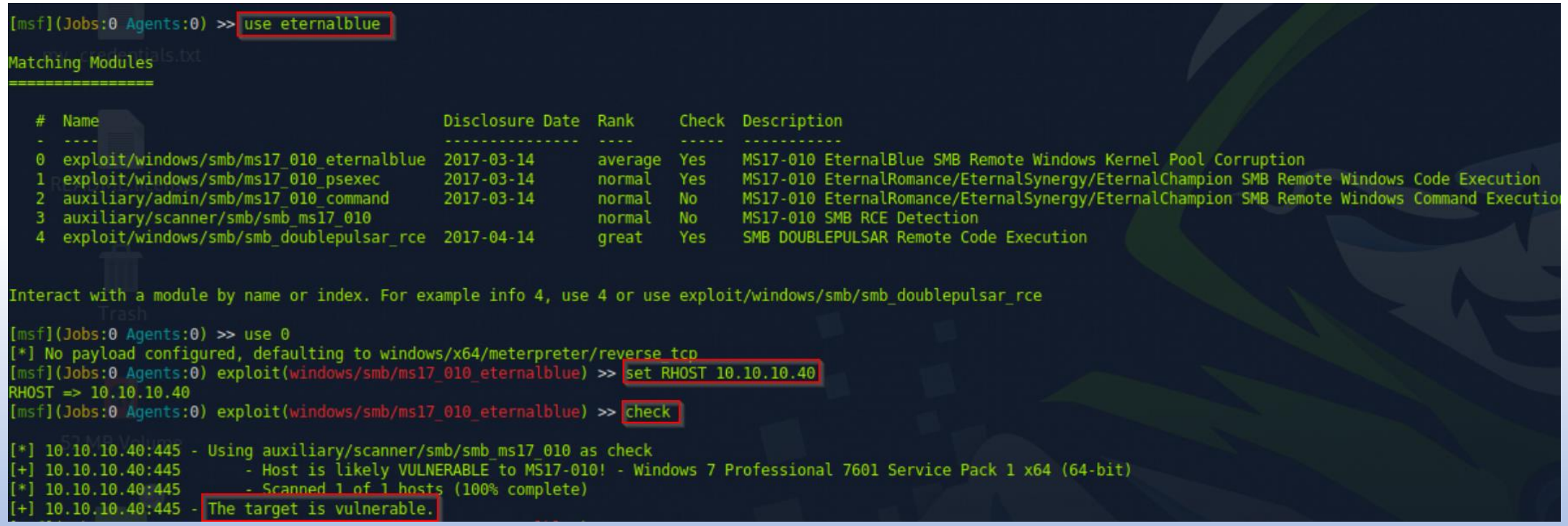
```
┌──[x]─[root@htb-ecsw3usj9e]─[/home/htb-oxeeql]
└──#nmap 10.10.10.40 -sC
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 21:40 BST
Nmap scan report for 10.10.10.40
Host is up (0.11s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
| clock-skew: mean: -19m56s, deviation: 34m36s, median: 1s
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-06-23T21:40:18+01:00
| smb2-time:
|   date: 2023-06-23T20:40:19
|_  start_date: 2023-06-23T20:29:28
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

IM TEST
EXPLOITATION: METASPLOIT

- (Unglaublich großes) Framework, um Angriffe durchzuführen
- Bietet Recon-Module, Exploits, Post-Exploit-Tools, Payloads und mehr für alle gängigen Betriebssysteme
- Automatisiert Angriffe
- Entwickelt und gepflegt von Rapid7
- Das Beste: könnt ihr kostenlos benutzen

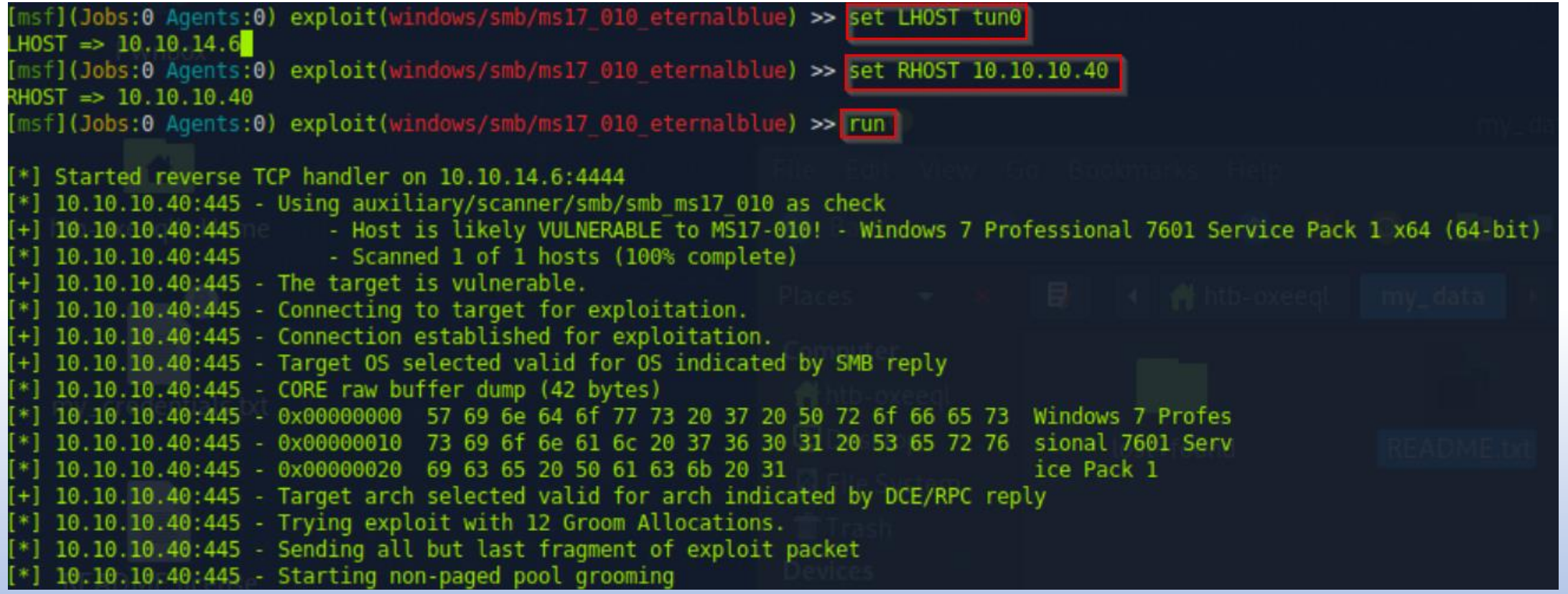


IM TEST
EXPLOITATION: METASPLOIT

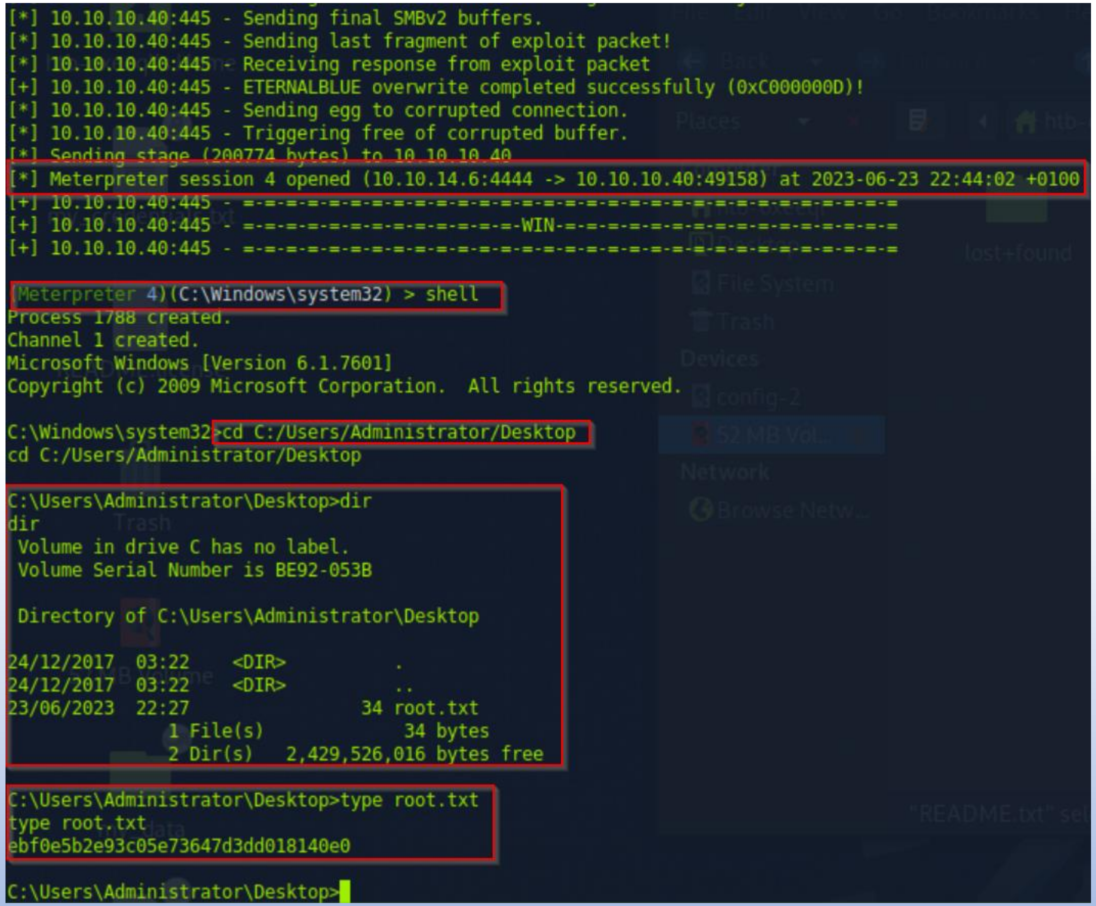


IM TEST

EXPLOITATION: METASPLOIT



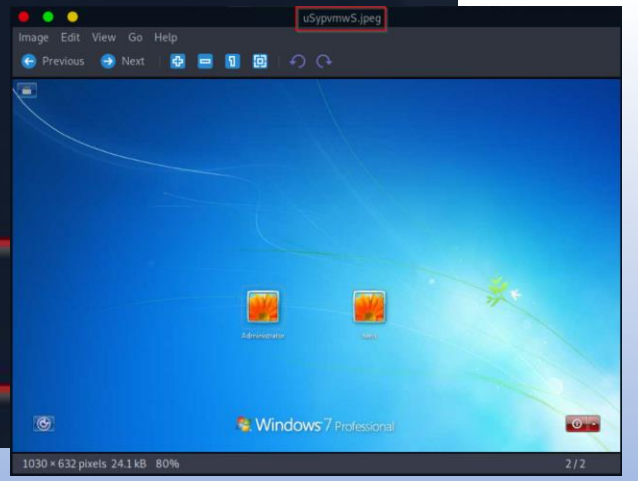
IM TEST
POST EXPLOITATION: METASPLOIT



IM TEST

POST EXPLOITATION: METASPLOIT

```
(Meterpreter 5)(C:\Windows\system32) > shell
Process 2892 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>exit
exit
(Meterpreter 5)(C:\Windows\system32) > screenshot
Screenshot saved to: /home/htb-oxeeql/uSypvmwS.jpeg
(Meterpreter 5)(C:\Windows\system32) >
```

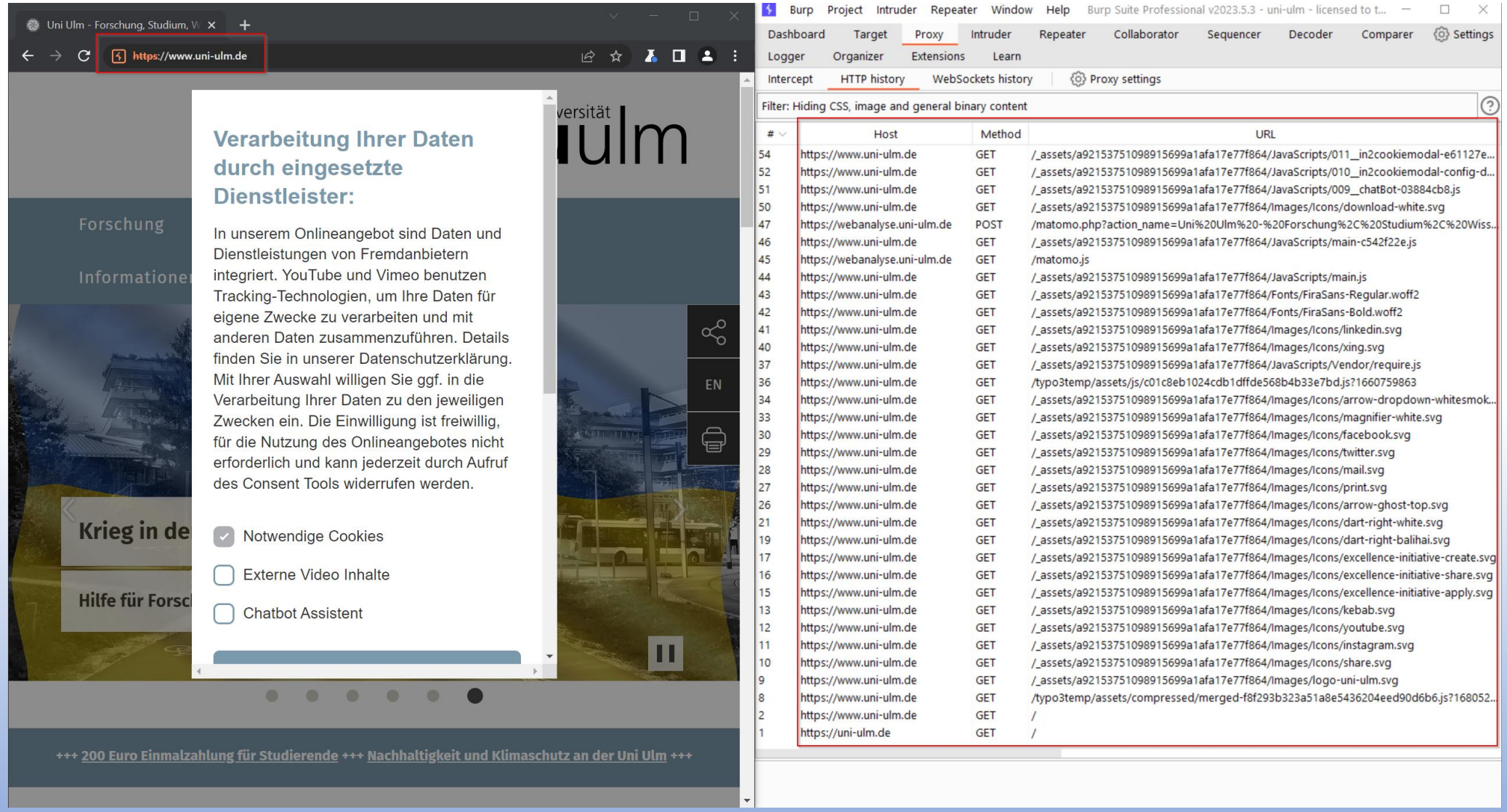


IM TEST
BURP SUITE – INTERCEPTION PROXY

- Interception Proxy
- Deutsch: Schaltet sich zwischen Browser und Webseite
- Ermöglicht Bearbeitung von Anfragen
- Beispiel-Ziel: User-Input da hin bekommen, wo/wie Entwickler ihn nicht erwartet

IM TEST

BURP SUITE- INTERCEPTION PROXY



IM TEST
BURP SUITE- INTERCEPTION PROXY

- [Demo Lab]
- Lab: https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-broken-logic

NACH DEM TEST BERICHT...

- In der Dokumentationsphase werden die Sachverhalte in einem Bericht erfasst s
- Die Schwachstellen müssen verständlich beschrieben sein, die Risiken klar erkennbar
- Empfehlungen sind auch Bestandteil unserer Arbeit
  - Dies ist nicht immer vollumfassend möglich, oft sind interne Abhängigkeiten nicht ersichtlich

NACH DEM TEST BERICHT...

- Wie "schlimm" ist eine Schwachstelle?
- Im Pentest wird jede Schwachstelle einzeln bewertet. Mögliche Bewertungen:
  - Eigene Einschätzung des Prüfers - auch nach Rücksprache mit den Systemverantwortlichen
    - Was sollte einfließen:
      - Ausnutzbarkeit: Wie einfach ist die Schwachstelle auszunutzen? Welche Voraussetzungen gibt es?
      - Potenzieller Schaden: Was ist der potenzielle Schaden?
  - Standards
    - z.B. CVSS (Common Vulnerablity Scoring System)

NACH DEM TEST
SCHWACHSTELLENBEWERTUNG: CVSS

- CVSS bietet einheitliche Bewertungsmöglichkeit von Schwachstellen
- Liefert qualitative und quantitative Bewertung einer Schwachstelle
- "Score" / Ergebnis: 0 – 10.0
- Aktuell CVSS v3.1
- Ab 01.10.2023: CVSS v4.0

CVSS v3.1 Score	Rating
0.0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

NACH DEM TEST
SCHWACHSTELLENBEWERTUNG: CVSS CALCULATOR

- Calculator siehe https://www.first.org/cvss/calculator/3.1
- Bewertung EternalBlue
- Bewertung Broken PW Reset

NACH DEM TEST
SCHWACHSTELLENBEWERTUNG: SORTIERUNG

Schwachstelle	CVSS v3.1
Eternalblue	9.8
Broken Password Reset	8.8
…	…

CTF VS ECHTES LEBEN

- CTF: Capture the Flag – Systeme, die aufgesetzt wurden, um sie zu ownen
- Beim CTF weiß man, dass es geht, also sucht man weiter, bis man es gefunden hat
- In echt muss man mit der Zeit haushalten
- CTFs beinhalten oft konstruierte Schwachstellen
- CTFs haben weniger "noise", man hat meist nur eine Hand voll Ansatzpunkte
- Echter Infra Test: 1000 IPs, 10000 Services

LUST AUF MEHR?

- cstehle@it-sec.de (bis 09/2023) | christian.stehle@mind-bytes.de (ab 10/2023)
- CTF-Plattformen zum Austoben:
  - https://www.hackthebox.com/ (Ihr müsst eine Challenge schaffen, damit ihr euch registrieren könnt)
  - PortSwigger WebSecurity Academy
- Bug Bounty – z.B. Hackerone oder BugCrowd
- Für Jobsuche: Zertifizierungen

  OSCP - Das bekannteste Zert, wird quasi immer anerkannt und respektiert (Infra, Web, Active Directory, OSINT, BufferOverflow) (1599$)

  Burp Suite Certified Practitioner - relativ unbekannt, aber inhaltlich exzellent (Nur Web) (89€)

  CRTO - mittelmäßig bekannt, inhaltlich exzellent (Active Directory, Red Team) (365£)