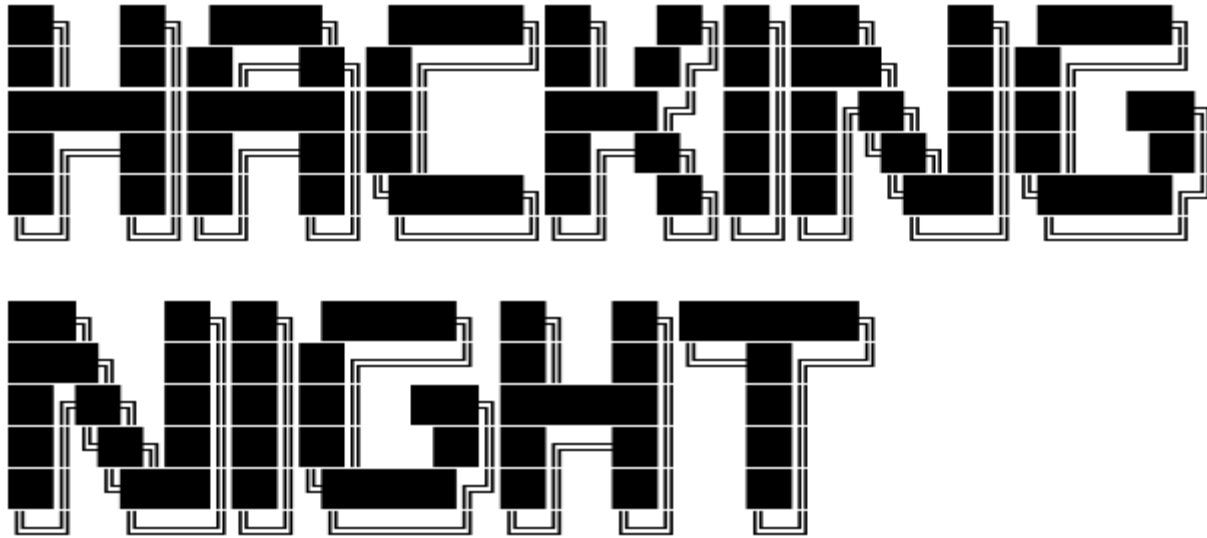
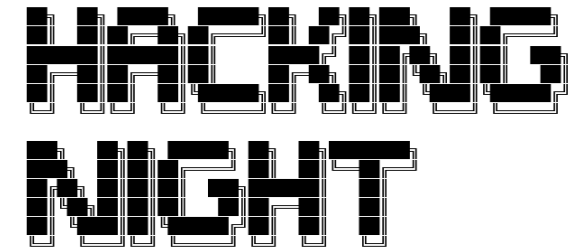


0x01 – Hacking Night, Onsite Meetup @ Rossi Lokal Gockhausen



HACKTHEBOX

Agenda



19.00 Uhr

Türöffnung

19.30 Uhr

Begrüßung und Setup

20.00 – 22.30 Uhr

Workshop Praxisteil

22.30 – 23.00 Uhr

Abschluss und Abschied

Admin

- Wi-Fi
- Toilets
- Pictures ok/nok?
- Hungry for pizza?

Dieci.ch

TWINT your name & order to Oli

Hosts



Antoine Neuenschwander
Tech Lead Bug Bounty Swisscom



Michel Neven
Founder Minesco, Data Engineer



Olivier Widmer
Senior Cyber Defense Officer
Swisscom

Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology

Acknowledge there is no 100% security

Find Vulnerabilities

Contradict all Assumptions



Legal Aspects

Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

Unauthorised access to a data processing system

Hack The Box

Provides lab environment to learn about attacker tactics



Gamification

Capture the Flag (CTF)

Hacking Competition

(warning: addictive)

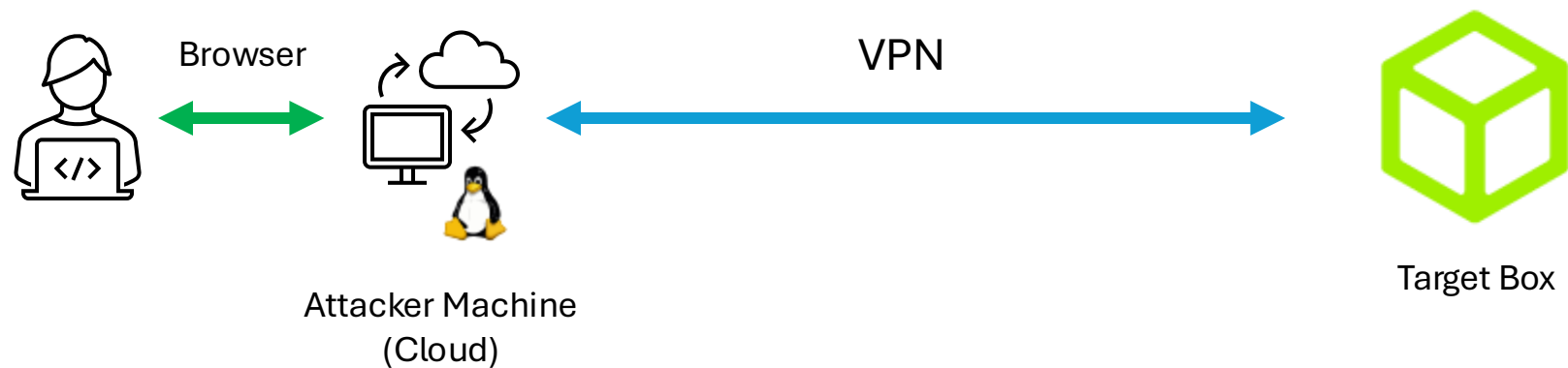
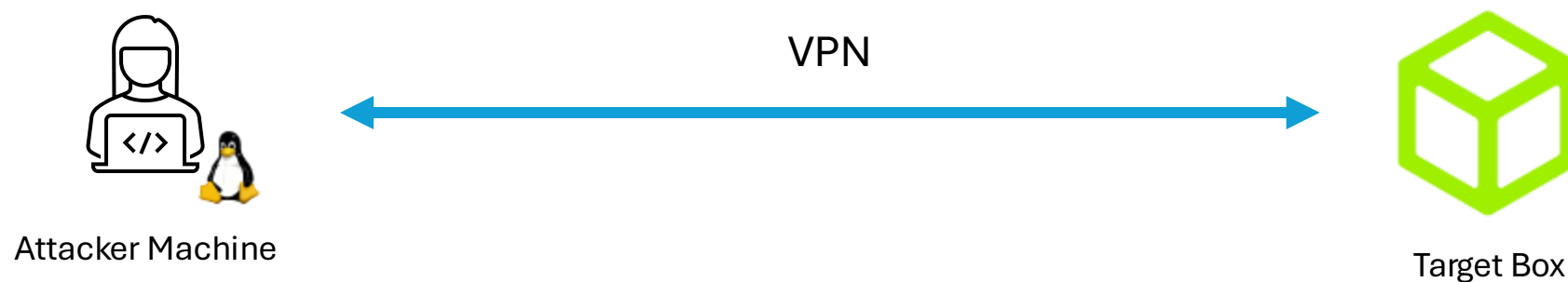




HACKTHEBOX

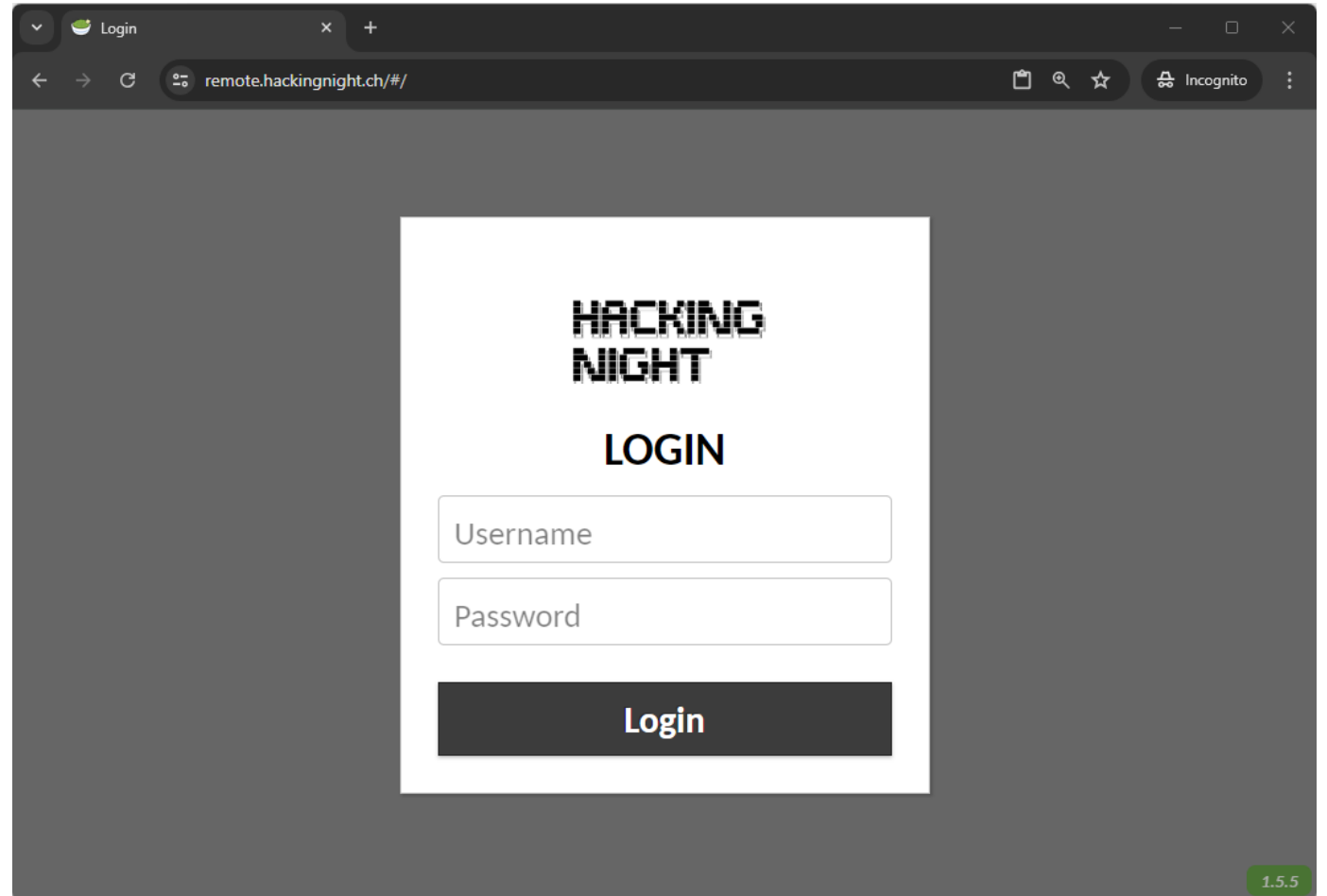
419 virtual machines (boxes)

Hacking Setup



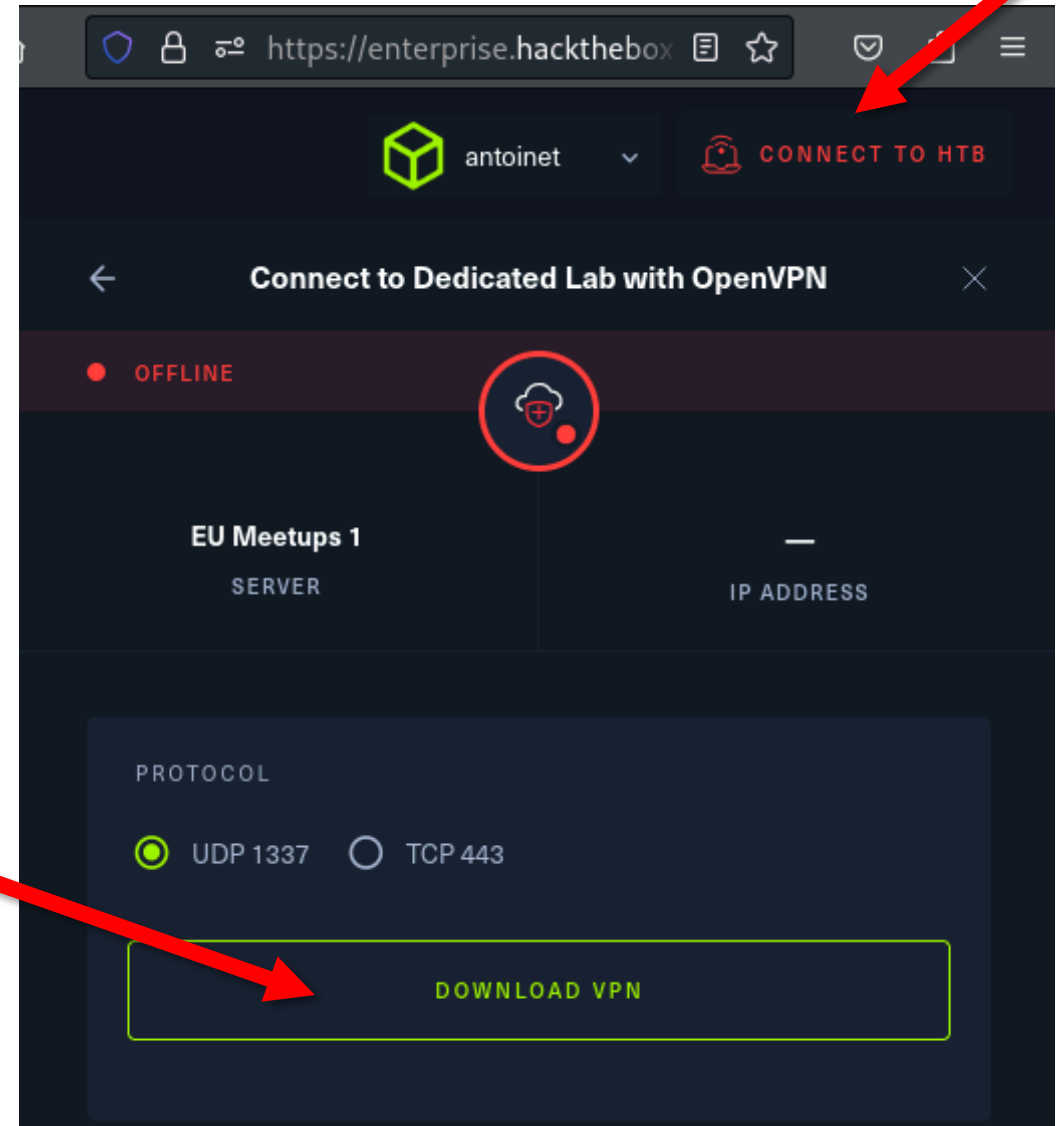
Connection to Attacker Machine

1. Visit remote.hackingnight.ch
2. Login with username **kali-X**
3. Password **hackingnight-X**



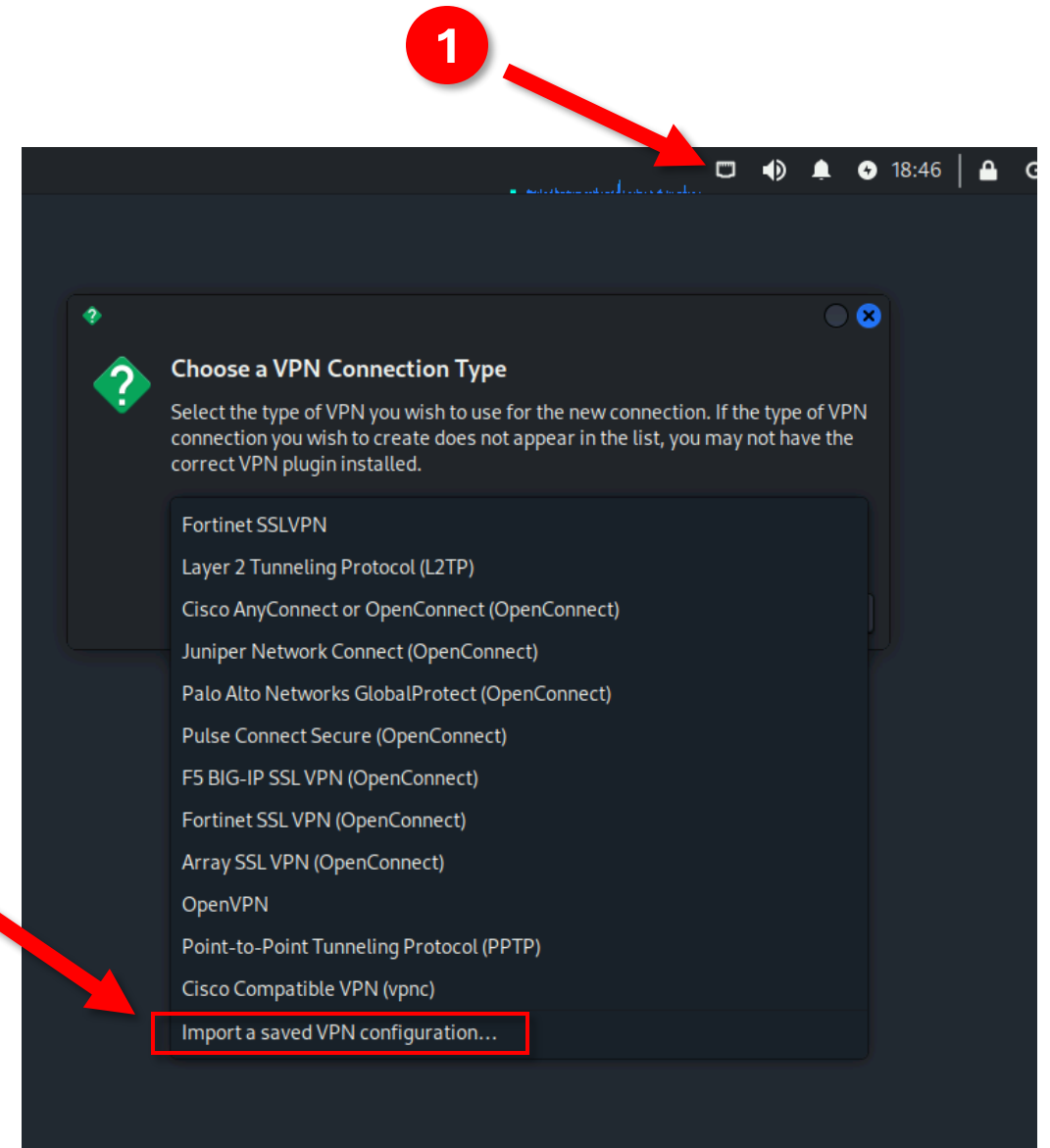
Configure VPN - Step 1

Download VPN profile



Configure VPN - Step 2

Import VPN profile



Tips for the Browser-Based VM

- @-Symbol:
 - Alt-Gr = Ctrl-Alt
 - Ctrl-Alt 2
- Copy-Paste from the Host:
 - Press Ctrl-Alt-Shift
 - Paste or copy selection in the text field

Cap

- Easy difficulty Linux machine
- HTTP server using non-encrypted traffic
- Insecure Direct Object Reference (IDOR)
- Exposed credentials can be used to login as a normal user
- Privilege escalation allows to login as root



Exploitation Steps

1. Network Scanning & Service Enumeration
2. Web Application Security
3. Network Trace Analysis
4. Privilege Escalation

#1 Network Scanning & Service Enumeration

Application

Provides **network services** to applications

HTTP, FTP, SMTP, SSH, etc.

Transport

Ensures **reliable data transfer** between devices

TCP Port
1337

Internet

Routing of data packets within and between networks

IP Address
203.0.113.45

Network Access

Physical Transmission of Data

- Ethernet (LAN cable)
- Wi-Fi

MAC Address
48:2C:6A:1E:59:3F




TCP Ports

Numerical identifiers used to distinguish different services on a host.

16bit range from 0-65535

Service	No	Description
HTTP	80	Web traffic
HTTPS	443	Secure web traffic
FTP	20/21	File transfer
SSH	22	Secure shell access
SMTP	25	Email sending



Service Enumeration using nmap

nmap = the network mapper

`nmap <IP address>`

example:

`nmap 10.11.12.240`

#2 Web Application Security

IDOR Vulnerability

- Insecure Direct Object Reference
- Manipulate numeric IDs in URLs or API calls



<https://onba.zkb.ch/konto/172271/>

#3 Network Trace Analysis

Wireshark

2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Info
4	0.011947	10.10.10.245	10.10.14.42	FTP	88	Response: 220 (vsFTPd 3.0.3)
6	0.019898	10.10.14.42	10.10.10.245	FTP	84	Request: USER anonymous
8	0.019979	10.10.10.245	10.10.14.42	FTP	102	Response: 331 Please specify the password.
10	1.098707	10.10.14.42	10.10.10.245	FTP	79	Request: PASS asdf

Frame 6: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.10.14.42, Dst: 10.10.10.245
Transmission Control Protocol, Src Port: 59634, Dst Port: 21, Seq: 3030
File Transfer Protocol (FTP)
 USER anonymous\r\n
 Request command: USER
 Request arg: anonymous
 [Current working directory:]

0000 00 00 00 01 00 06 00 50 56 b9 03 7c 00 00 08 00P V...|..
0010 45 10 00 44 60 0d 40 00 3f 06 ae 64 0a 0a 0e 2a E..D`.@.?.d..
0020 0a 0a 0a f5 e8 f2 00 15 20 bb 9c ff 0a 46 9f 8bF..
0030 80 18 7f f6 bc 37 00 00 01 01 08 0a 9d 12 59 e27...F..
0040 64 55 d9 89 55 53 45 52 20 61 6e 6f 6e 79 6d 6f dU..USER anony
0050 75 73 0d 0a us..

Gaining Foothold

- Use the discovered credentials (username/password) on other services
- Password Re-use
- Examples:
 - File Transfer Protocol (ftp)
 - Secure Shell (ssh)
- Hint: *client application* is usually named after the *protocol* itself

Capture the Flag

- Retrieve the value of the flag located in `/home/user/flag.txt`

#4 Privilege Escalation

Privilege Escalation

- We have **foothold as a normal user**
- Goal: escalate privileges to gain **administrative privileges** on the machine
- Windows: Local Administrator
- Linux: root

Capture the flag under /root/flag.txt

Linux User IDs / Filesystem Attributes

Run "id" to retrieve current user id:

- Normal user: 1000
- Root: 0

```
$ ls -la /usr/bin/ping
```

```
-rwxr-xr-x 1 root root 76672 Feb 5 2022 /usr/bin/ping
```

setuid permission

Allows a process to run with the privileges of the file owner

setuid bit

-swxr-xr-x 1 root root



setuid capability

\$ getcap myprogram

myprogram cap_setuid+pe

Privilege Escalation

- Find a program with **setuid** permission
- Run it
- You will automatically have root privileges

LinPEAS

- **Linux Privilege Escalation Awesome Script**
- **Goal:**
 - Enumerate file permissions and configurations
 - Find known exploitable patterns that allow to escalate to root
- **Instructions:**
 - Google: "linpeas"
 - Download script
 - Execute
 - Win

Capture the (root) flag

- Ok, you can run the program as root...
- ...but how do you make the program read/output the flag under /root/flag.txt?



Award Ceremony

Acknowledgements

Many Thanks!

- Michel & Oli
- Team Rossi Lokal
- Quartiersverein Gockhausen



Thanks for your Participation ! You did Awesome !!!

Check out the Meetup Page for next events:

- 18.07.2024 Sphères Zurich
- 29.08.2024 Sphères Zurich
- 26.09.2024 Sphères Zurich



HACKTHEBOX