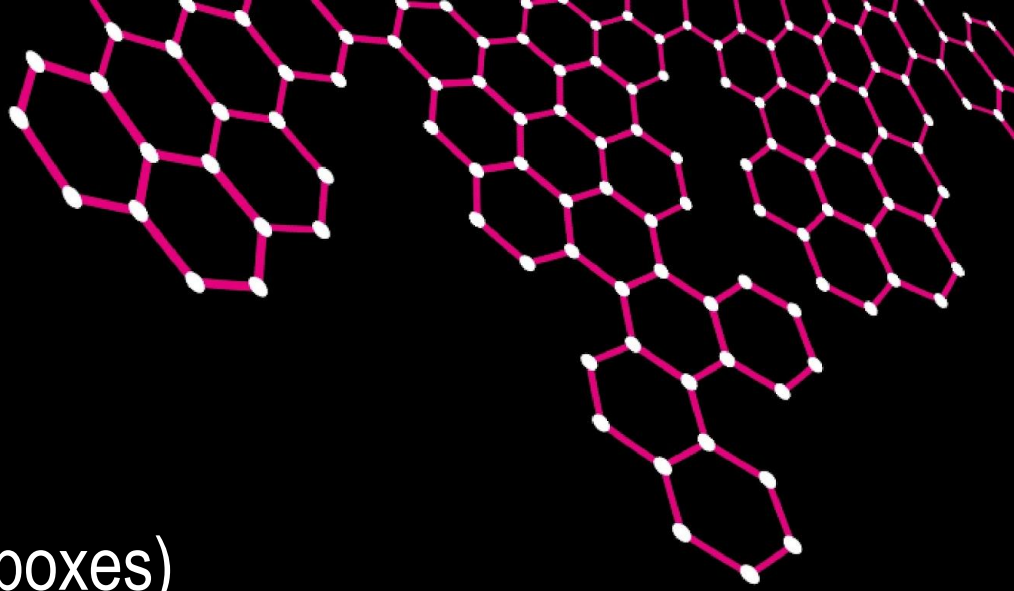
UNIVERSITY OF TWENTE.



THS - Hacking live machines (boxes)

Thijs van Ede (t.s.vanede@utwente.nl)

Attacking machines

- The goal: Exfiltrate secret data (FLAG) from another computer

Attacking machines

- The goal: Exfiltrate secret data (FLAG) from another computer
- The problem:
  - We do not own the other machine

Attacking machines

- The goal: Exfiltrate secret data (FLAG) from another computer
- The problem:
  - We do not own the other machine
  - We (often) need root access to read the FLAG file

Attacking machines

- The goal: Exfiltrate secret data (FLAG) from another computer
- The problem:
  - We do not own the other machine
  - We (often) need root access to read the FLAG file
- The solution: We pwn the other machine 😈

Attacking machines - How?

- Follow the cyber kill chain

Attacking machines - How?

- Follow the cyber kill chain
  - Microsoft STRIDE

Attacking machines - How?

- Follow the cyber kill chain
  - Microsoft STRIDE
  - Lockheed Martin Cyber Kill Chain

Attacking machines - How?

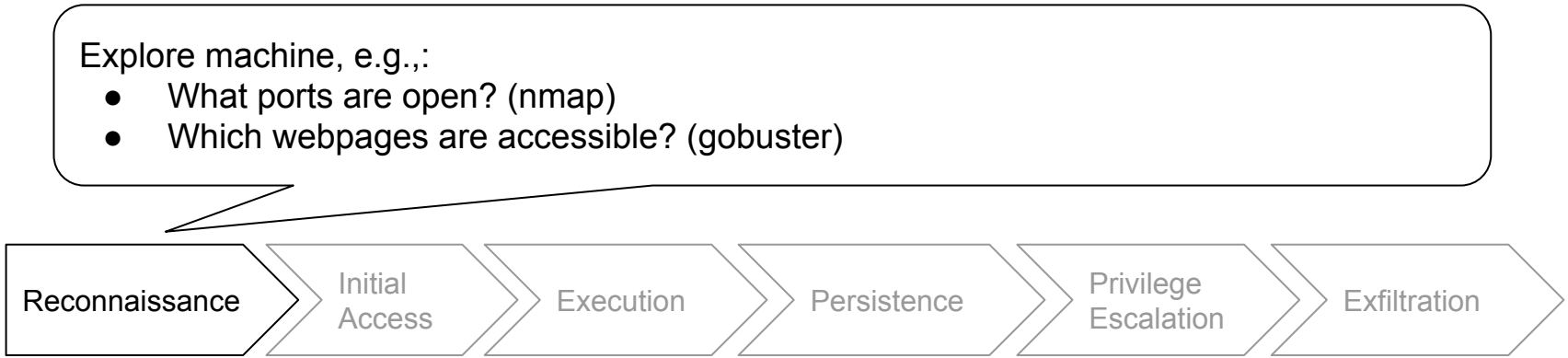
- Follow the cyber kill chain
  - Microsoft STRIDE
  - Lockheed Martin Cyber Kill Chain
  - Mitre ATT&CK

Attacking machines - How?

- Follow the cyber kill chain
  - Microsoft STRIDE
  - Lockheed Martin Cyber Kill Chain
  - Mitre ATT&CK
- Often, in attacking machines we need to take the following steps:

Attacking machines - How?

- Follow the cyber kill chain
  - Microsoft STRIDE
  - Lockheed Martin Cyber Kill Chain
  - Mitre ATT&CK



Attacking machines - How?

- Follow the cyber kill chain
  - Microsoft STRIDE
  - Lockheed Martin Cyber Kill Chain
  - Mitre ATT&CK

Access the (public) interfaces of the machine, e.g.,:
- Login to the webpage / create account
- Play around with the environment / explore ways to inject commands

Attacking machines - How?

- Follow the cyber kill chain
  - Microsoft STRIDE
  - Lockheed Martin Cyber Kill Chain
  - Mitre ATT&CK

Execute commands:
- Find ways to execute commands (direct execution / PHP injection / etc.)
- Try to get shell access (reverse shell)

Attacking machines - How?

- Follow the cyber kill chain
  - Microsoft STRIDE
  - Lockheed Martin Cyber Kill Chain
  - Mitre ATT&CK

Execute commands:
- Stabilize shell / get ssh access
- (Optional) Add backdoors in e.g. startup scripts / cronjobs to keep upon reboot

Attacking machines - How?

- Follow the cyber kill chain
  - Microsoft STRIDE
  - Lockheed Martin Cyber Kill Chain
  - Mitre ATT&CK

Gain root access:
- Find vulnerable applications / scripts on machine (linPEAS)
- Exploit privilege escalation vulnerabilities (Metasploit)

Attacking machines - How?

- Follow the cyber kill chain
  - Microsoft STRIDE
  - Lockheed Martin Cyber Kill Chain
  - Mitre ATT&CK

Obtain the FLAG:
- Can often be found in the `/root` directory
- Submit FLAG for points

Demo time!

TryHackMe - Pickle Rick room
(https://tryhackme.com/room/picklerick)

Attacking machines - Reconnaissance

- NMAP
  - Scan IP address / domain name for open ports
  - `nmap <IP/domain>`

Attacking machines - Reconnaissance

- NMAP
  - Scan IP address / domain name for open ports
  - `nmap <IP/domain>`

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-22 15:53 CET
Nmap scan report for ths.eemcs.utwente.nl (130.89.7.191)
Host is up (0.0072s latency).
Not shown: 939 filtered ports, 58 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 3.82 seconds
```

Attacking machines - Reconnaissance

- Gobuster
  - Scan common pages on website
  - `Gobuster dir -w <wordlist> -u <IP/domain> -x <extensions>`

Attacking machines - Reconnaissance

- Gobuster
  - Scan common pages on website
  - `Gobuster dir -w <wordlist> -u <IP/domain> -x <extensions>`

```
===============================================================
2021/11/22 15:57:06 Starting gobuster in directory enumeration mode
===============================================================
/index.html               (Status: 200) [Size: 612]
/resources                (Status: 301) [Size: 0] [--> /resources/]
/admin                    (Status: 301) [Size: 0] [--> /admin/]
/static                   (Status: 301) [Size: 178] [--> https://ths.eemcs.utwente.nl/static/]
Progress: 2200 / 1764488 (0.12%)
```

Attacking machines - Initial Access

- Varies widely per machine
  - Interact with website

Attacking machines - Initial Access

- Varies widely per machine
  - Interact with website
  - Brute-force usernames / passwords

Attacking machines - Initial Access

- Varies widely per machine
  - Interact with website
  - Brute-force usernames / passwords
- Hydra
  - Brute force common usernames and passwords
  - `hydra -l <username> -P <password_list_file> <IP/domain> ssh`
  - `hydra -L <username_list_file> -p <password> <IP/domain> ftp`

Attacking machines - Execution

- Obtain a reverse shell

Attacking machines - Execution

- Obtain a reverse shell
- Problem:
  - The server firewall (often) blocks incoming connections, however we can send outgoing connections

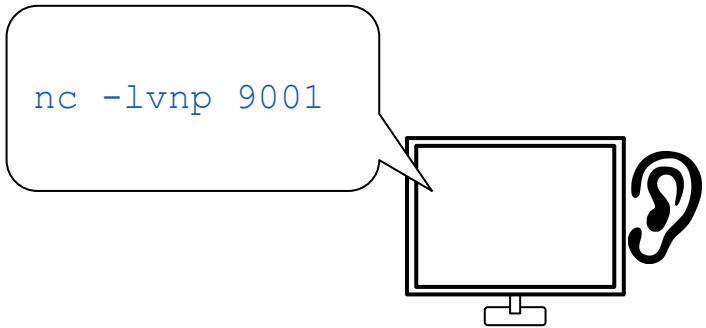
Attacking machines - Execution

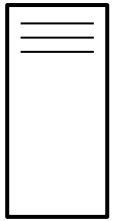
- Obtain a reverse shell
- Problem:
  - The server firewall (often) blocks incoming connections, however we can send outgoing connections
- Solution:
  - Listen on our own computer for incoming connections (netcat: `nc -lvnp 9001`)

Attacking machines - Execution

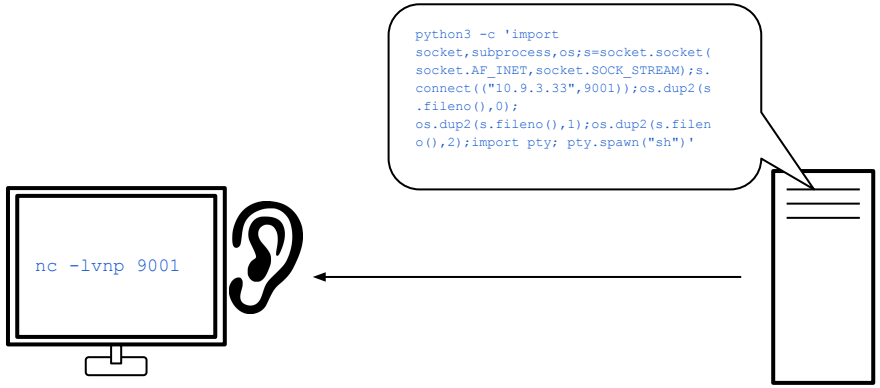
- Obtain a reverse shell
- Problem:
  - The server firewall (often) blocks incoming connections, however we can send outgoing connections
- Solution:
  - Listen on our own computer for incoming connections (netcat: `nc -lvnp 9001`)
  - Make server initiate reverse shell (https://www.revshells.com/)

Attacking machines - Execution



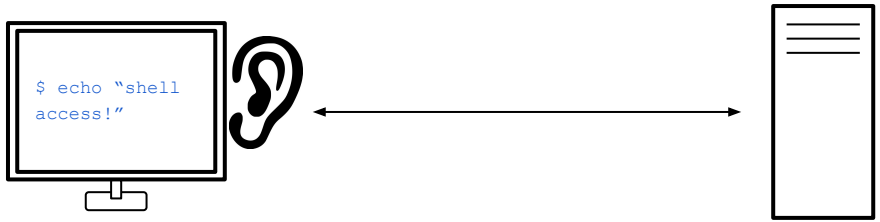


Attacking machines - Execution



Reconnaissance | Initial Access | **Execution** | Persistence | Privilege Escalation | Exfiltration

Attacking machines - Execution



Attacking machines - Persistence

- The current shell is not stable

Attacking machines - Persistence

- The current shell is not stable
- Stabilize shell for features such as
  - Autocomplete
  - Previous commands

Attacking machines - Persistence

- The current shell is not stable
- Stabilize shell for features such as
  - Autocomplete
  - Previous commands

Bash

```
python3 -c "import pty; pty.spawn(\"/bin/bash\")"
# Press ctrl+z (put current shell in background mode)
stty raw -echo
fg
export TERM=xterm
```

Attacking machines - Persistence

- The current shell is not stable
- Stabilize shell for features such as
  - Autocomplete
  - Previous commands

Zsh

```
python3 -c "import pty; pty.spawn(\"/bin/bash\")"
# Press ctrl+z (put current shell in background mode)
stty raw -echo; fg
stty rows $LINES cols $COLUMNS
export TERM=xterm-256color
exec /bin/bash
```

Attacking machines - Privilege escalation

- linPEAS
  - Search for possible paths to escalate privileges on Linux/Unix*/MacOS hosts
    https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

Attacking machines - Privilege escalation

- linPEAS
  - Search for possible paths to escalate privileges on Linux/Unix*/MacOS hosts https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS
  - Also available for Windows (https://github.com/carlospolop/PEASS-ng)

Attacking machines - Privilege escalation

- linPEAS
  - Search for possible paths to escalate privileges on Linux/Unix*/MacOS hosts https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS
  - Also available for Windows (https://github.com/carlospolop/PEASS-ng)

linpeas.sh

```
User www-data may run the following commands on
ip-10-10-119-213.eu-west-1.compute.internal:
      (ALL) NOPASSWD: ALL
```

Attacking machines - How?

- Search the system for FLAGs
  - User flags are often in `/home/<username>`
  - Root flags are often in `/root`

Try it yourself!

- Challenges
  - TryHackMe - Basic Pentesting (https://tryhackme.com/room/basicpentestingjt)
  - TryHackMe - OWASP Top 10 (https://tryhackme.com/room/owasptop10)
  - https://hackthebox.eu → Labs → Machines
  - See https://ths.eemcs.utwente.nl/resources