# Linux 2 DEVOPS 2020
# Lektion 11

# Idag

- Redovisningar av gruppuppgift
- På begäran: Härdning
- Repetitionsövningar

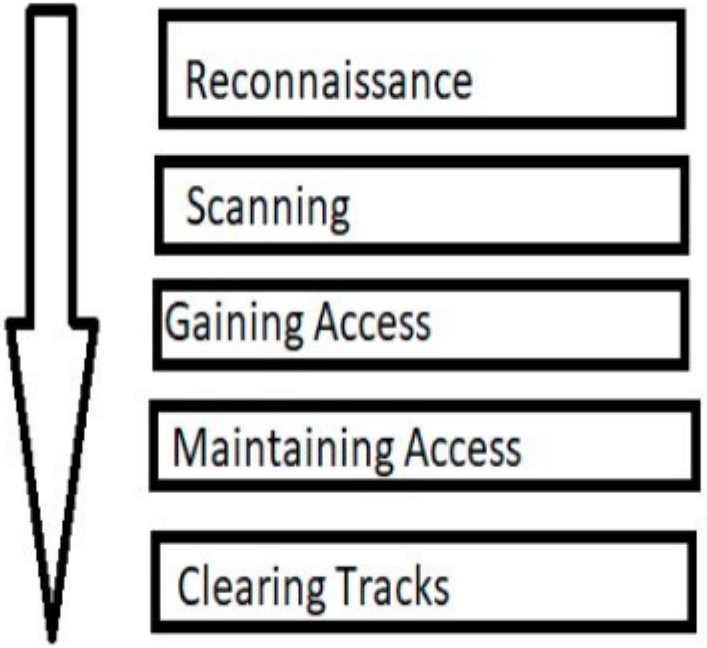
# Redovisningar

Plats på scen för gruppredovisningarna

# Härdning

- Vad skall servern vara till för?
- Vad behöver vi skydda?
- Vilka är riskerna?
- Hitta och täppa till svagheter.

# Generell hackingprocess




Skiss stulen från
https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking

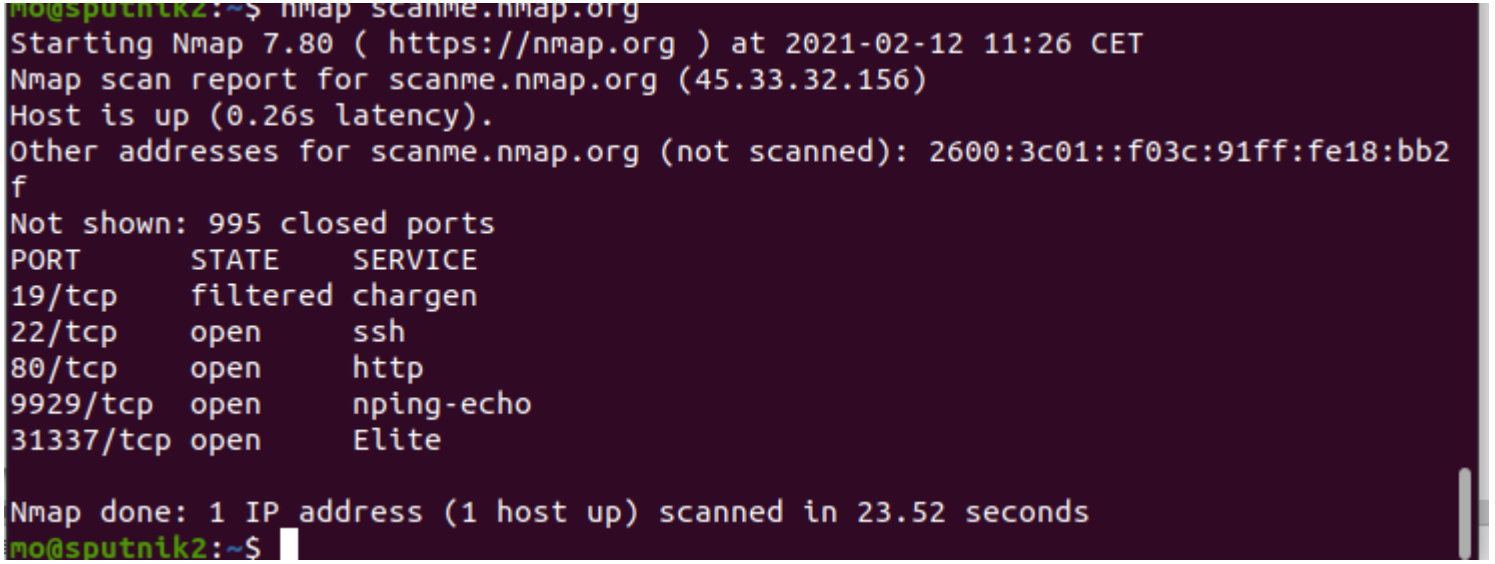
# Ta sig in

- Identifiera tjänster som är igång
  - nmap
  - Wireshark
- Hitta vägar in
- Exploatera för att få högre behörigheter

# Övning 1

- Använd nmap för att scanna någon lämplig server, t ex scanme.nmap.org
  - Paketet för apt heter nmap

# Övning 1: nmap



# Basal säkerhet

- Inga osäkra protokoll
- Ingenting igång som inte behöver vara igång

# Säkrade inloggningar

- ssh med nyckel (PKI) istället för lösenord
- Tvinga fram lösenordsbyten var 30:e dag
- Lära folk att använda unika lösenord

# ssh med nyckel

- Generera nyckelpar

```
ssh-keygen -t rsa -b 4096 -C "email@domain.com"
```

- Kopiera den publika nyckeln till servern din användare skall logga in till

```
ssh-copy-id remote_username@server_address
```

- Exempel med varje steg:

  https://linuxize.com/post/how-to-setup-passwordless-ssh-login/

# Säkra konfiguration av ssh

- Konfig-fil /etc/ssh/sshd_config
- Ingen inloggning direkt som root:

  PermitRootLogin no
- Ingen inloggning med lösenord, dvs endast med nycklar:

  PasswordAuthentication no

# Övning 2

- Ta en titt på din /etc/ssh/sshd_config
- Om den tillåter inloggning som root, slå av det

# OWASP top ten

- Håll särskild koll på riskerna i OWASP top 10

  https://owasp.org/www-project-top-ten/

# OWASP top ten

1. Injection
   - Se till att programmen är ordentligt skrivna med bing-variabler
2. Broken authentication
   - Koll på hur inloggningar kan ske
3. Sensitive data exposure
   - Koll på vad ni visar för data, inte minst på webbsiter
4. XML External Entities (XXE)
   - Använd inte gamla protokoll

# OWASP top ten

5. Broken Access Control
   - Kontroll är ordet
6. Security Misconfiguration
   - Säkerhet är alltid ett pågående arbete
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

# Repetitionsövningar

# Övning R1

- Gör ett skript som tar ett directorynamn som inparameter
- Om detta directory inte existerar, skall skriptet skapa det och lägga dit en fil med namnet ”new”
- Om detta directory redan existerar, skall skriptet skriva en tidsstämpel i slutet av en fil som heter ”last” i directoryts

# Övning R1

```
#!/bin/bash

dir=$1;

if [ ! -d $dir ]
then
    mkdir $dir;
    touch $dir/new;
else
    timestamp=`date +%Y-%m-%d_%H-%M-%S`;
    echo $timestamp >>$dir/last
fi
```

# Övning R2

- Skapa ett program som med tjugo sekunders mellanrum skriver en tidsstämpel och ”hej” till en loggfil
- Efter 30 rader byter den namn på denna loggfil till en fil med samma namn plus ”.bak”, och fortsätter sedan med ny loggfil
- Gör en service av programmet och kör denna

# Övning R2

```
#!/bin/bash

log=logfile;
i=0;

while true
do
    i=$((i+1));
    timestamp=`date +%Y-%m-%d_%H-%M-%S`;
    echo $timestamp ": hej" >>$log;
    if [ $i == 30 ]
    then
       mv $log $log.bak;
       i=0;
    fi
    sleep 20;
done
```

# Övning R2

```
[Unit]
Description=Simple service

[Service]
User=mo
WorkingDirectory=/var/scripts
ExecStart=/var/scripts/r2d
Restart=always

[Install]
WantedBy=multi-user.target
```

# Övning R3

- Implementera följande:

  Två gånger i timmen kontrolleras ifall eth0 är uppe, och resultatet skrivs till en log-fil, med tidsstämpel

# Övning R3

```
#!/bin/bash

Logfile=/var/log/myiptest.log;
timestamp=`date +%Y-%m-%d_%H-%M-%S`;

ip a | grep eth0 | grep "state UP" >/dev/null;
if [ $? -eq 0 ];
then
   echo $timestamp ": eth0 UP" >>$logfile;
else
   echo $timestamp ": eth0 DOWN" >>$logfile;
fi
```

Till crontab:

```
0,30 * * * *  /var/scripts/iptest.sh
```

# Övning R4

- Ta reda på vilka mailservrar som finns konfigurerade för domänen nackademin.se
- Se om det går att kontakta dessa på standardporten för SMTP

# Övning R4

dig mx nackademin.se

```
;; ANSWER SECTION:
nackademin.se.          14400   IN   MX 10 nackademin-se.mx1-se.mailanyone.net.
nackademin.se.          14400   IN   MX 20 nackademin-se.mx2-se.mailanyone.net.
nackademin.se.          14400   IN   MX 30 nackademin-se.mx3-se.mailanyone.net.
```

```
telnet nackademin-se.mx1-se.mailanyone.net 25
Trying 185.38.181.4...
Connected to nackademin-se.mx1-se.mailanyone.net.
Escape character is '^]'.
```

# Tillbakablick, reflektion, kommentarer ...