Linux 2 DEVOPS 2020
Lektion 5

Idag

- Säkerhet och nätverkssäkerhet
- Säkerhetstänkande och riskbedömningar på olika nivåer
- iptables
- Härdning

Säkerhet på många nivåer

- Veta vem som skall ha tillgång till vad
- Skalskydd (koll på fysisk tillgång)
- Värdering av tillgångar
- Medvetande och kunskap inom organisationen
- IT-säkerhet

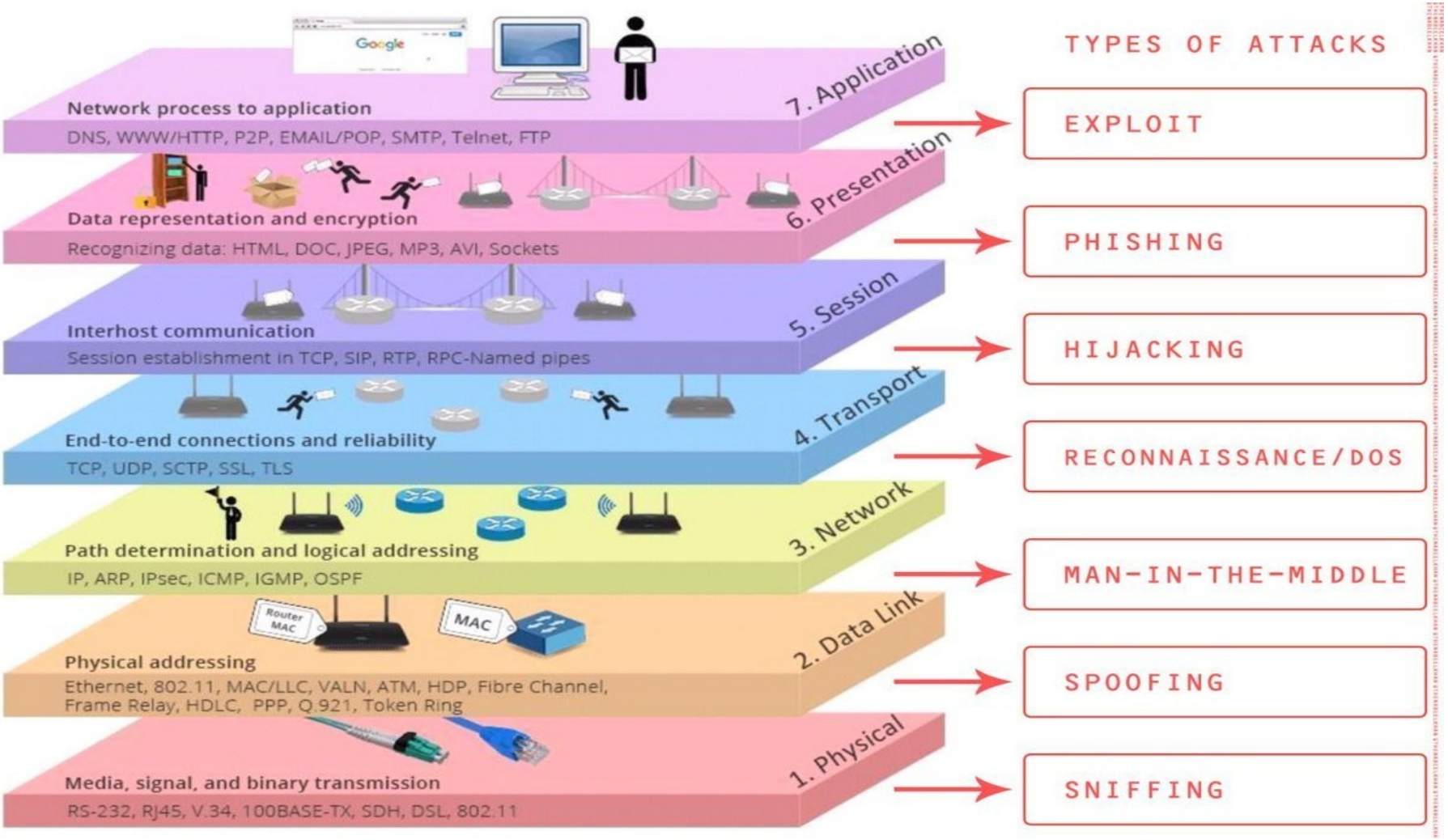
Veta vad man vill skydda och varför man vill skydda det

- Vad är värdet?
- Vilka är riskerna?
- Vad är det värt att skydda det här?

IT-säkerhet

- Driftsäkerhet – att systemen är uppe när de förmodas vara uppe, tillräckligt stabila etc
- Dataskydd – att endast behöriga kommer åt uppgifter
- Tillförlitlighet – att de uppgifter som finns i systemet är korrekta

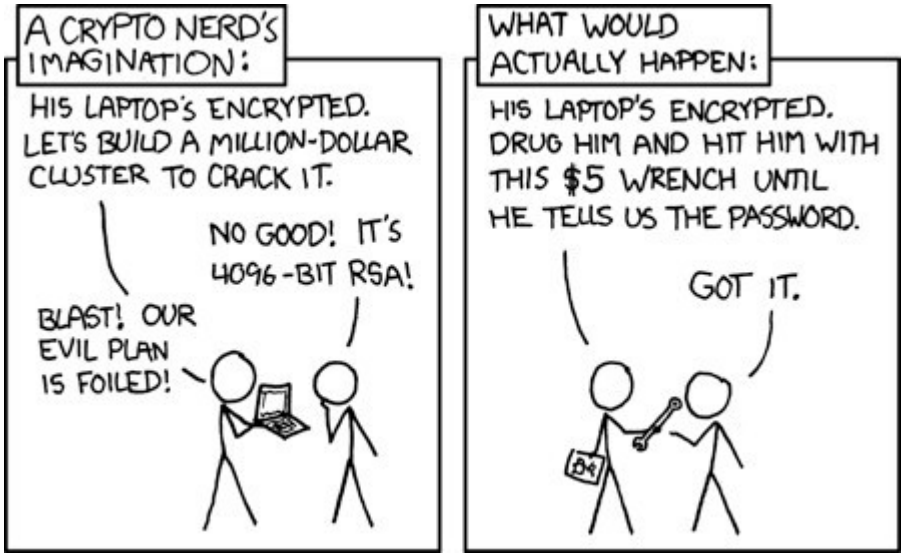
Attack


TYPES OF ATTACKS
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
EXPLOIT
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
PHISHING
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
HIJACKING
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
RECONNAISSANCE/DOS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
MAN-IN-THE-MIDDLE
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
SPOOFING
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
SNIFFING

Social engineering

- Tekniska lösningar kan inte avhjälpa mänskliga svagheter
- Vaksamhet på rätt nivå
- Veta vem som får tillgång till vad

Se realistiskt på de faktiska riskerna



Från xkcd av Randall Munroe, xkcd.com

Risker

- Gå igenom riskerna kring ett system
  - Vad kan hända här?
- Värdera
  - Hur troligt är det att det händer?
  - Hur allvarligt är det om det händer?
- Besluta om åtgärder för att riskerna skall anses vara på acceptabel nivå

Exempel på riskanalys

Risk	Sannolikhet	Konsekvens	Riskvärde	Åtgärder
Skriver fel	5	1	5 (låg)	-
Datorexplosion	4	5	20 (hög)	Andra datorer
Sladd ur	2	4	8 (låg)	-

Övning 1

- Hitta så många risker ni kan komma på för genomförande av en kurs på Nackademin
- Värdera riskerna
- Föreslå åtgärder för risker med riskvärde >=10

Övning 1, exempel

Risk	Sannolikhet	Konsekvens	Riskvärde	Åtgärder
Oklar kursplan	3	4	12	Klargöranden
Ingen lärare	3	5	15	Säkrad tillgång
Teknikproblem	4	1	4	-
Sjuk student	3	4	12	Material på nät
Inställd lektion	2	2	4	-

Tekniska lösningar på tekniska problem

- Nätverk – vad behöver vara öppet
  - Bra brandväggar
  - Avdelade nätverk
  - Skilja på internt nät och DMZ
- Ordentligt modulär och flerskiktat arkitektur
- Tillräckligt stark autentisering
- Kryptering

Nätverkssäkerhet

- Brandväggar
  - Vad skall vara öppet?
  - Behöver trafiken övervakas?
- iptables
  - Linux-program som fungerar som inbyggd brandvägg
  - Filtrera vad som får komma in respektive komma ut

iptables

- ”chain” som reglerar en väg för nätverkstrafik
- Policy på chain-nivå
- Tabeller, för olika sorters nätverkstrafik
  - En tabell innehåller chains
- Defaulttabellen är att man ställer in filter, men kan också användas för annat
- Kan t ex även användas för NAT (annan tabell)

Övning 2

- Uppvärmning iptables:

  Se hur din lokala iptables ser ut just nu med

  `iptables -l`

- Lägg märke till vilka tre (troligen) chains du ser i defaulttabellen filter

iptables

- Tom filter-tabell:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

iptables default chains

- `PREROUTING` : Packets will enter this chain before a routing decision is made.
- `INPUT` : Packet is going to be locally delivered. It does not have anything to do with processes having an opened socket; local delivery is controlled by the "local-delivery" routing table: `ip route show table local` .
- `FORWARD` : All packets that have been routed and were not for local delivery will traverse this chain.
- `OUTPUT` : Packets sent from the machine itself will be visiting this chain.
- `POSTROUTING` : Routing decision has been made. Packets enter this chain just before handing them off to the hardware.

Från wikipedia

iptables

- Innehåller en uppräkning / tabell av regler
- Reglerna kontrolleras i tur och ordning tills någon matchar den trafik det gäller
- Lägg till regel med iptables -A
- Ta bort regel med iptables -D
- Lägg till regel på specifik plats i tabellen med iptables -I

iptables

- Tillåt all trafik:

```
iptables -A [INPUT | OUTPUT] ACCEPT
```

- Blockera all trafik:

```
iptables -A [INPUT | OUTPUT] DROP
```

- Blockera inkommande trafik från en viss adress:

```
iptables -A INPUT -s <BLOCK_IP> -j DROP
```

iptables exempel

- Tillåt ssh från specifikt nätverk:

  iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

  iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

- Tillåt all inkommande http:

  iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

  iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT

- Tillåt forward från ett nätverk till ett annat (ofta internt till externt):

  iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

iptables exempel

- Stäng för utgående trafik på http-porten:

  iptables -A OUTPUT -p tcp --dport 80 -j DROP
- Tillåt trafik ut till specifikt nätverk:

  iptables -A OUTPUT -p tcp -d nackademin.se -j ACCEPT
- Stäng för all trafik in:

  iptables -P INPUT DROP
- Stäng för all trafik ut:

  iptables -P OUTPUT DROP
- Rensa tabellen helt:

  iptables -F
- En trevlig samling exempel finns här:
  https://www.thegeekstuff.com/2011/06/iptables-rules-examples/

Övning 3

- Stäng av din egen Linux-maskins tillgång till en webbsite (t ex www.generationt.se) med iptables.
- Testa att blockeringen fungerar.
- Ta bort blockeringen igen.

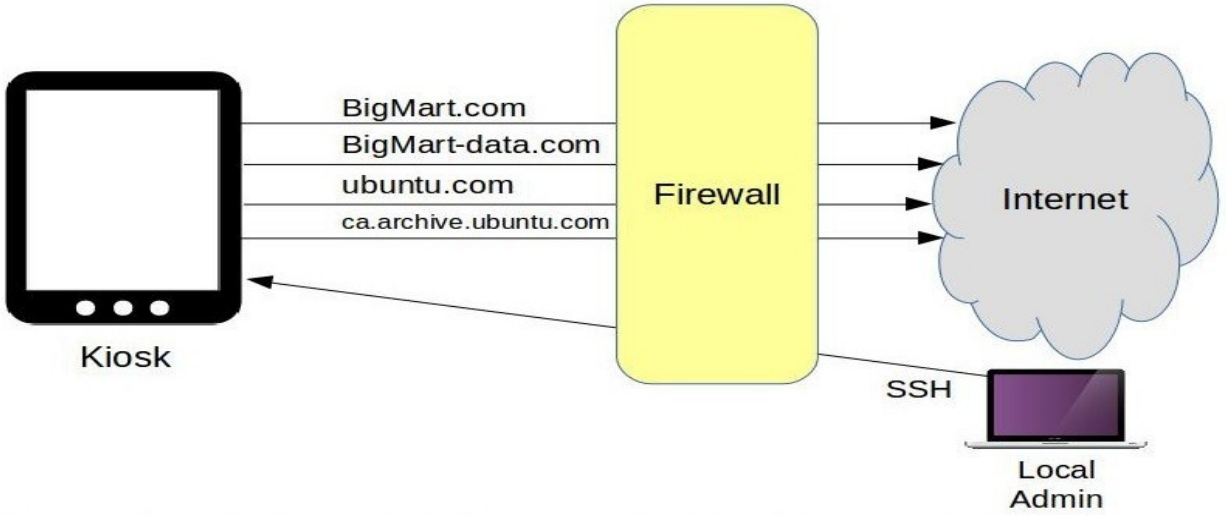
Övning 3

```
iptables -A OUTPUT -p -tcp -d www.generationt.se -j DROP
```

Övning 4

- Tänk dig att du gör iptables-konfigurationen för en ”kiosk” enligt bilden nedan. Skapa rätt iptables.

  Om du gör praktiska experiment på den maskin du har uppkopplad, tänk på att behålla öppet för Zoom också!



Övning 4

```
iptables -A OUTPUT -p tcp -d bigmart.com -j ACCEPT
iptables -A OUTPUT -p tcp -d bigmart-data.com -j ACCEPT
iptables -A OUTPUT -p tcp -d ubuntu.com -j ACCEPT
iptables -A OUTPUT -p tcp -d ca.archive.ubuntu.com -j ACCEPT
iptables -A OUTPUT -p tcp --dport 80 -j DROP
iptables -A OUTPUT -p tcp --dport 443 -j DROP
iptables -A INPUT -p tcp -s 10.0.3.1 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 0.0.0.0/0 --dport 22 -j DROP
```

Övningsexemplet stulet från
https://opensource.com/article/18/9/linux-iptables-firewalld

Härdning

- Vad skall finnas på just den här servern?
- Vem skall ha tillgång till just den här servern?
- Härdning: Se till att bara det som behöver vara öppet är öppet och att bara den som behöver tillgång får tillgång

Härdning: allmänna åtgärder

- Gå igenom listan över existerande daemoner / services

```
systemctl list-units --all
```

- Gå igenom listan över installerade paket

```
apt list --installed
```

- Ingen inloggning som root – använd sudo istället

```
sudo passwd -l root
```

Övning 5

- Gå igenom listan över existerande services på din maskin. Vilka av dem används idag?
- Gå igenom listan över installerade paket på din maskin. Vilka av dem använder du dig av?

Härdning: kommunikation

- Koll på öppna portar (brandvägg eller iptables)

```
iptables -L
netstat -a | grep tcp | grep LISTEN
```

- Undvik ftp m fl osäkra kommunikationssätt
  - Stäng relevanta portar
  - Undvik att ha ftpd igång
- Använd ssh, scp, sftp
  - För en webbserver även relevant att använda https snarare än http

Övning 6

- Gå igenom listan på öppna portar som lyssnar utåt på din maskin. Vet du vilka program de hör till?

Härdning: användare

- Plocka bort användarkonton som inte behövs

  `deluser <user>`

- Tvinga fram återkommande lösenordsbyten

  chage -M <maxdays> -m <mindays> -W <warn> <user>

  Exempel: `chage -M 60 -m 3 -W 7 testuser`

- Lås konto efter ett antal misslyckade inloggningsförsök

  använd pam_tally2 eller skript som tittar i faillog och räknar samt passwd -l för att låsa konto

Övning 7

- Skapa en testanvändare. Se vilka defaultvärden denne får för lösenordsbyten i /etc/shadow.
- Sätt nu att din testanvändare tvingas byta lösenord efter 30 dagar. Se hur värden i /etc/shadow ändrats.

Övning 7

- Defaultläge:

```
testuser1:$6$PQUyzmD6$7czwTU8PH8nbPUhR0sC/1MQu.tazzaF8b45aU15L5JwnoOa6BfTNdkSgqf
Evh3v9ldBMpzwOGgIxNDjOTNMnF/:18498:0:99999:7:::
```

- Efter chage -M 30 -m 3 -W 7 testuser1

```
testuser1:$6$PQUyzmD6$7czwTU8PH8nbPUhR0sC/1MQu.tazzaF8b45aU15L5JwnoOa6BfTNdkSgqf
Evh3v9ldBMpzwOGgIxNDjOTNMnF/:18498:3:30:7:::
```

Övning 8

- Antag att ni skall härda två Linuxservrar för drift. Nr1 skall användas som webbserver. Nr2 skall användas för en MySQL-databas som nr1 hämtar data från.
- Hur härdar ni respektive server? Gör en åtgärdslista för vardera (och testa gärna konkreta kommandon).

Övning 8

- Gemensamt för båda servrarna:
  - Öppet för ssh-trafik för övervakning / underhåll, i övrigt stängt för inkommande trafik förutom undantag nedan.
  - Minimalt antal användarkonton, enbart individuella konton tillåter inloggning, kontroll av sudo-rättigheter, tvinga fram regelbundna lösenordsbyten.
  - Ingenting igång som inte behöver vara igång.
- Nr1:
  - Öppet för http och https utifrån.
- Nr2:
  - Öppet för trafik till MySQL (port 3306) från server nr1.

Tillbakablick, reflektion, kommentarer ...