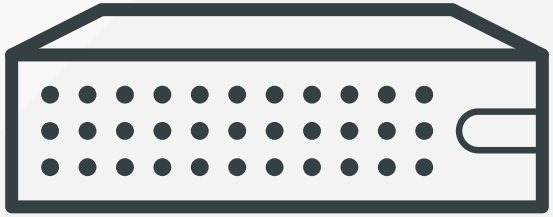
BEZPEČNOST SLUŽEB NA INTERNETU

ANEB JAK SE SCHOVAT

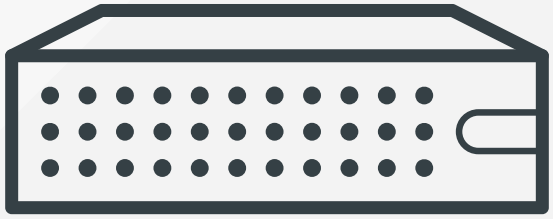
JAKUB JELEN
@JakujeCZ

OpenAlt, Brno, 2016

KDO Z VÁS PROVOZUJE SERVER?



JAKÉ VÁM NA NĚM BĚŽÍ SLUŽBY?



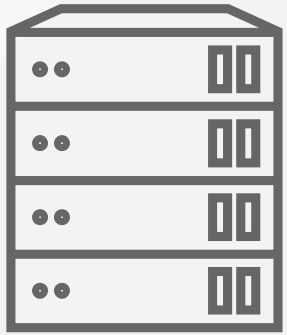
```
21/tcp   open   ftp   vsftpd 3.0.2
| ssl-cert: Subject: commonName=example.com/countryName=CZ
[...]
22/tcp   open   ssh   OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 f7:ea:35:4d:7e:60:b5:12:1d:79:ad:09:96:83:aa:35 (DSA)
[...]
25/tcp   open   smtp  Postfix smtpd
[...]
| ssl-cert: Subject: commonName=example.com/countryName=CZ
[..]
80/tcp   open   http  Apache httpd 2.4.10
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Did not follow redirect to https://example.com/
110/tcp  open   pop3  Dovecot pop3d
[...]
| ssl-cert: Subject: commonName=example.com/countryName=CZ
[...]
```

```
143/tcp  open     imap         Dovecot imapd
[...]
| ssl-cert: Subject: commonName=example.com/countryName=CZ
[...]
443/tcp  open     ssl/http     Apache httpd 2.4.10
[...]
| ssl-cert: Subject: commonName=www.example.com
[...]
465/tcp  open     ssl/smtp     Postfix smtpd
[...]
993/tcp  open     ssl/imap     Dovecot imapd
[...]
995/tcp  open     ssl/pop3     Dovecot pop3d
[...]
9001/tcp open     http         Node.js Express framework
| http-auth:
| HTTP/1.1 401 Unauthorized
|_  Basic realm=Protected Area
|_http-server-header: Etherpad 31452b2 (http://etherpad.org)
```

AGENDA

- Služby na Internetu
  - Veřejné x neveřejné
- Útoky na Internetu
  - Náhodné x cílené
- Ochrana služeb
  - Aktivní x pasivní
- Fwknop
  - Vlastnosti
  - Praktická ukázka skrytí SSH

SLUŽBY NA INTERNETU



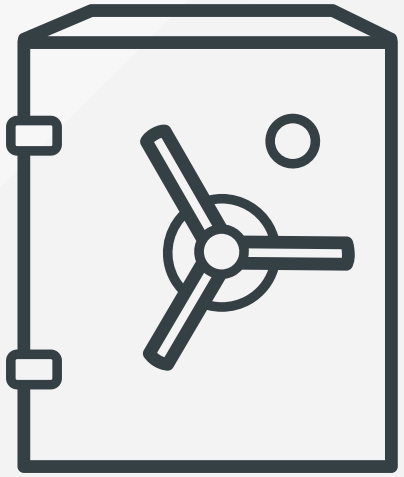
SLUŽBY NA INTERNETU

- Komunikace s okolím
- Veřejné
  - Mnoho předem neznámých uživatelů
  - Dostupnost
  - Web (HTTP(S))
  - Email (SMTP)
- Soukromé
  - Omezený počet uživatelů
  - Velké riziko zneužití
  - Správa serveru (SSH)
  - Email (IMAP)
  - Přenos souborů (FTP(S))

ÚTOKY NA INTERNETU

- Zneužití služby nebo serveru
- Náhodné
  - Sken portů
  - Hledání zranitelných verzí
  - Výchozí hesla
  - Pozdější cílení
- Cílené
  - Útok hrubou silou
  - Zranitelnosti (CVE)
    - Publikované
    - Neznámé
  - Stejná hesla z jiných služeb

OCHRANA SLUŽEB



OCHRANA SLUŽEB

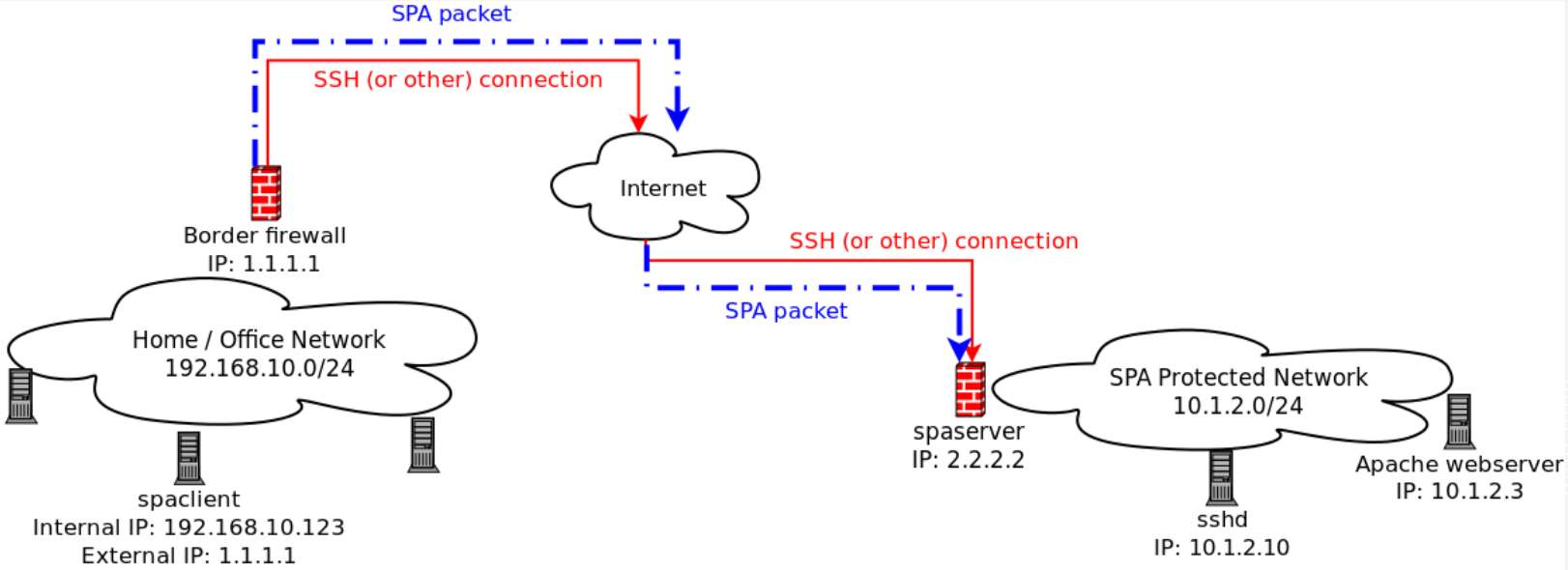
- Zajištění dostupnosti
  - autorizovaní uživatelé
- Odepření přístupu
  - útočníci
- Aktivní
  - Sledování logů
  - Blokování útočníků (dynamický blacklist)
  - Fail2ban (podpora IPv6), Logwatch
- Pasivní
  - Skrytí služby
  - Autorizace uživatelů (whitelist)
  - port knocking, **fwknop**

```
---------------------- fail2ban-messages Begin ------------------------


Banned services with Fail2Ban:                              Bans:Unbans
   postfix:                                                    [  5:1  ]
   ssh:                                                        [314:304]

----------------------- fail2ban-messages End -------------------------
```

FWKNOP


SPA packet
SSH (or other) connection
Internet
Border firewall
IP: 1.1.1.1
SSH (or other) connection
SPA packet
Home / Office Network
192.168.10.0/24
spaserver
IP: 2.2.2.2
SPA Protected Network
10.1.2.0/24
Apache webserver
IP: 10.1.2.3
spaclient
Internal IP: 192.168.10.123
External IP: 1.1.1.1
sshd
IP: 10.1.2.10

FWKNOP

- Skrytí služby
  - Obrana proti všem útokům
  - Není náhrada silných hesel!
- Autorizace pro otevření portu
  - Jak se chrání fwknop?
- UDP port: neviditelné pro scan
- Jediný paket:
  - Neopakovatelný
  - Šifrovaný AES
  - Integrita HMAC SHA256
- 2 klíče
  - Symetrický/Asymetrický
  - HMAC

PRAKTICKÁ UKÁZKA

- Vytvoření klíčů (klient)

```
[client]$ fwknop -A tcp/22 -a 192.168.122.1 -D 192.168.122.49 \
    --key-gen --use-hmac --save-rc-stanza
[*] Creating initial rc file: /home/jakuje/.fwknoprc.
[+] Wrote Rijndael and HMAC keys to rc file: /home/jakuje/.fwknoprc
[client]$ cat /home/jakuje/.fwknoprc
[192.168.122.49]
ALLOW_IP                    192.168.122.1
ACCESS                      tcp/22
SPA_SERVER                  192.168.122.49
KEY_BASE64                  PNfH+6kdbsoy/Hixd8vP8hs+5bTrCrAsREoZ++lCwM4=
HMAC_KEY_BASE64             mkqxxJQvVqnOwzL4dFiTuconvXi/s876IFBRXn9b[...]==
USE_HMAC                    Y
```

PRAKTICKÁ UKÁZKA

- Uložení klíče na server

```
[client]$ cat /home/jakuje/.fwknoprc

[192.168.122.49]
ALLOW_IP                        192.168.122.1
ACCESS                          tcp/22
SPA_SERVER                      192.168.122.49
KEY_BASE64                      PNfH+6kdbsoy/Hixd8vP8hs+5bTrCrAsREoZ++lCwM4=
HMAC_KEY_BASE64                 mkqxxJQvVqnOwzL4dFiTuconvXi/s876IFBRXnb9[...]==
USE_HMAC                        Y

[server]$ cat /etc/fwknop/access.conf

SOURCE                          ANY
KEY_BASE64                      PNfH+6kdbsoy/Hixd8vP8hs+5bTrCrAsREoZ++lCwM4=
HMAC_KEY_BASE64                 mkqxxJQvVqnOwzL4dFiTuconvXi/s876IFBRXnb9[...]==
```

PRAKTICKÁ UKÁZKA

- Spuštění démona a ověření funkčnosti

```
[server]$ systemctl enable fwknop && systemctl start fwknop
 Ubuntu: START_DAEMON="yes" v /etc/default/fwknop-server
[client]$ fwknop -n 192.168.122.49
[server]$ journalct -b -e
[...] SPA Packet from IP: 192.168.122.1 received with access source match
```

- Služba stále viditelná (mnoho informací):

```
[client]$ nmap -A -T4 192.168.122.49
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; prot. 2.0)
| ssh-hostkey:
|   2048 eb:2d:e8:fa:37:3b:50:42:a2:64:5c:47:7b:b8:9f:12 (RSA)
|_  256 c5:db:49:5b:6d:40:e1:17:3f:72:c2:74:b0:42:3b:85 (ECDSA)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

PRAKTICKÁ UKÁZKA

- Skrytí služby za firewall (default drop policy):

```
[server]$ firewall-cmd [--permanent] --remove-service=ssh
```

```
 Ubuntu: # iptables -I INPUT 1 -p tcp --dport 22 -j DROP
         # iptables -I INPUT 1 -p tcp --dport 22 -m conntrack \
             --ctstate ESTABLISHED,RELATED -j ACCEPT
```

- Služba je skrytá

```
[client]$ nmap -A -T4 192.168.122.49
```

```
Not shown: 999 closed ports
PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
```

PRAKTICKÁ UKÁZKA

- Připojení ke skryté službě

```
[client]$ ssh 192.168.122.49
ssh: connect to host 192.168.122.41 port 22: No route to host
ssh: connect to host 192.168.122.41 port 22: Connection timed out
```

- Po zaslání SPA paketu

```
[client]$ fwknop -n 192.168.122.49
[client]$ ssh 192.168.122.49
[server]$ journalctl -b -e
[...] SPA Packet from IP: 192.168.122.1 received with access source match
[...] Added access rule to FWKNOP_INPUT for 192.168.122.1 -> 0.0.0.0/0 tcp/
22, expires at 1476002511
[...] Removed rule 1 from FWKNOP_INPUT with expire time of 1476002511
```

KAM DÁLE?

- Umíme skrýt SSH server za firewall.
- Stejným způsobem lze skrýt jakoukoliv jinou službu
  - `fwknop --access tcp/port`
  - Omezení portů na serveru (blacklist, whitelist)
- Lze spouštět obecné příkazy na serveru
  - `echo "ENABLE_CMD_EXEC Y" >> /etc/fwknop/access.conf`
  - `fwknop --server-cmd "echo hello > /tmp/test"`
- Použití asymetrické kryptografie (GPG)
  - omezení velikosti klíče velikostí ethernet paketu
- Grafické nástroje:
  - Fwknop-gui
  - Android, iPhone aplikace
- Problémy -- blokování a filtrování provozu (UDP)

OTÁZKY?