FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

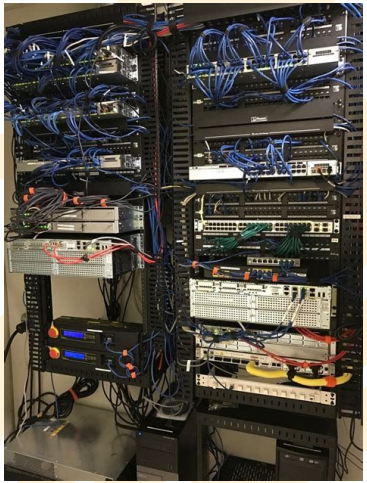
Firewall a obrana proti (síťovým) útokům

Ing. Tomáš Čejka, Ph.D.
Laboratoř monitorování síťového provozu, FIT ČVUT v Praze

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Síťová infrastruktura - propojení strojů

- Domácí počítač / notebook / mobil / tablet / server / skupina serverů - cluster
  dnes dokonce už i televize / lednička / pračka / kávovar / …
- Kabely - metalické / optické
  Bezdrátové spoje - elektromagnetické záření (může být světlo, nebo pomalejší mikrovlnné záření)
- Síťové prvky - přepínač (switch) a směrovač (router)
  … nebo obojí dohromady
  Pro bezdrátové sítě “přístupový bod” (access point)
  … nebo všechno dohromady.



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

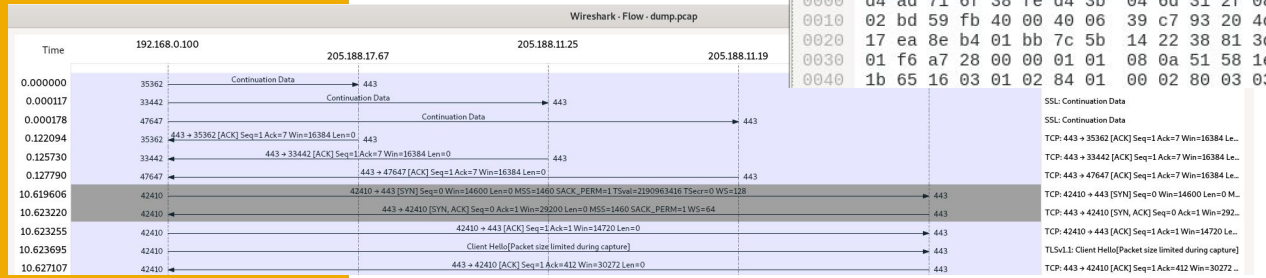
Síťová komunikace - co to je?

- Paket
- Směrování paketů
  (“jak je možné, že se zpráva doručí tam, kam má?”)
- Adresace

No.	Time	Src Port	Source	Destination	Dst Port	Protocol
1	2021-03-12 12:08:03,5103641…	36532	147.32.76.…	172.217.23…	443	TLSv1
2	2021-03-12 12:08:16,7091409…	57626	147.32.76.…	3.123.248.…	443	TLSv1
3	2021-03-12 12:08:16,7301129…	48228	147.32.76.…	3.123.217.…	443	TLSv1
4	2021-03-12 12:08:17,4784124…	38660	147.32.76.…	18.194.78.…	443	TLSv1
5	2021-03-12 12:08:17,5455141…	38664	147.32.76.…	18.194.78.…	443	TLSv1
6	2021-03-12 12:08:17,7008761…	49182	147.32.76.…	199.232.16…	443	TLSv1
7	2021-03-12 12:08:18,4264574…	60050	147.32.76.…	3.233.54.64	443	TLSv1

```
▸ Frame 1: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface wlo1,
▸ Ethernet II, Src: IntelCor_6d:31:2f (d4:3b:04:6d:31:2f), Dst: Cisco_6f:38:fe (d4:ad:71:6f
▸ Internet Protocol Version 4, Src: 147.32.76.149, Dst: 172.217.23.234
▸ Transmission Control Protocol, Src Port: 36532, Dst Port: 443, Seq: 1, Ack: 1, Len: 649
▸ Transport Layer Security
```

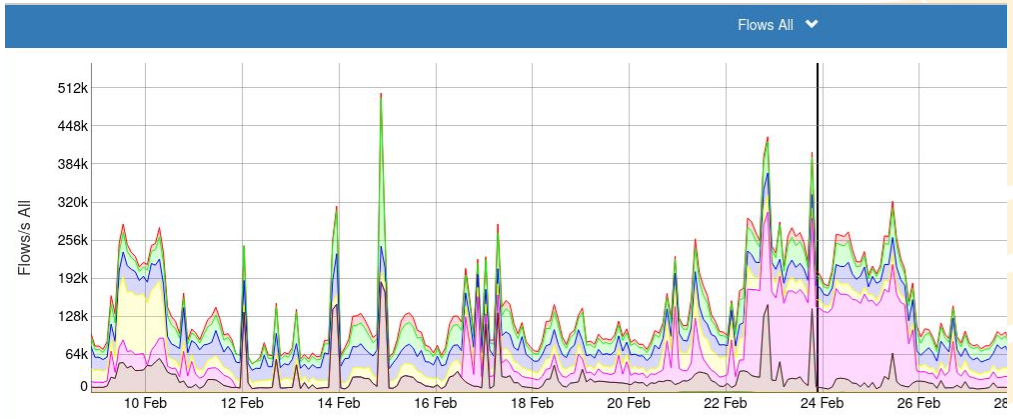
```
0000  d4 ad 71 6f 38 fe d4 3b  04 6d 31 2f 08 00 45 00   ··qo8··;  ·m1/··E·
0010  02 bd 59 fb 40 00 40 06  39 c7 93 20 4c 95 ac d9   ··Y·@·@·  9·· L···
0020  17 ea 8e b4 01 bb 7c 5b  14 22 38 81 3d 2c 80 18   ·····|[·  ·"8·=,··
0030  01 f6 a7 28 00 00 01 01  08 0a 51 58 1e 0b bd dc   ···(····  ··QX····
0040  1b 65 16 03 01 02 84 01  00 02 80 03 03 7b 32 f2   ·e····  ····{2·
```



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Nežádoucí komunikace :-(

- Útočník se snaží přihlásit (hádání přihlašovacích údajů hrubou silou, “brute-force”)
- Útočník pošle nebezpečnou zprávu (zneužití zranitelnosti aplikace, “vulnerability exploit”)
- Útočník odesílá víc než dokážeme přijmout (naše “linka” má omezenou kapacitu, “Distributed Denial of Service” - DDoS)



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

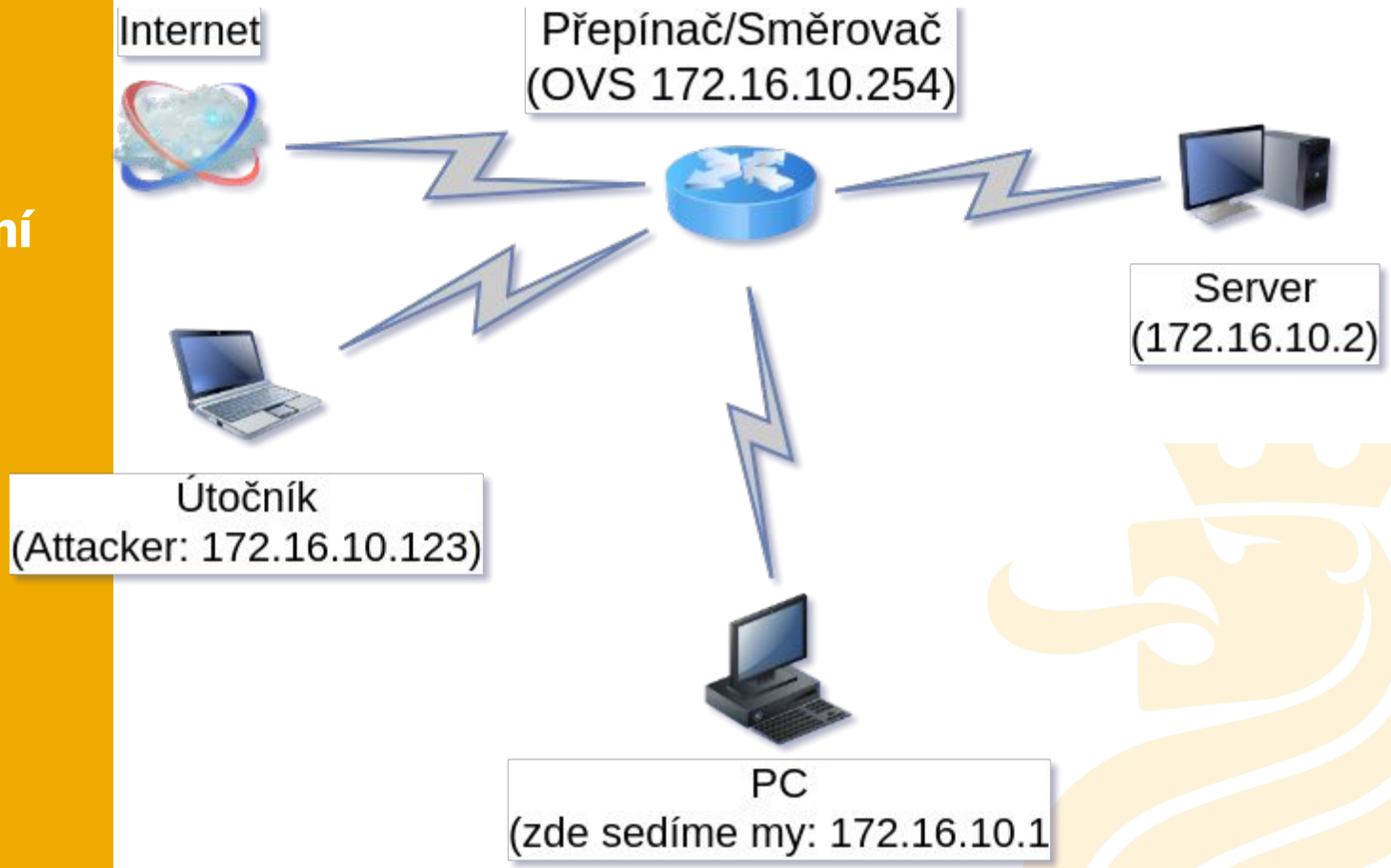
Firewall

- Nástroj, který umí kontrolovat pakety (nebo posloupnosti souvisejících paketů)
- A dokáže s pakety provádět “operace” (například ZAHODIT paket)
- 1) Podmínka, která se kontroluje,
  2) Akce, která se provede

```
cejkat@fedora:~
1112:~$ sudo firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: wlo1
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
1112:~$ sudo firewall-cmd --list-all --zone=trusted
trusted
  target: ACCEPT
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
1112:~$
```

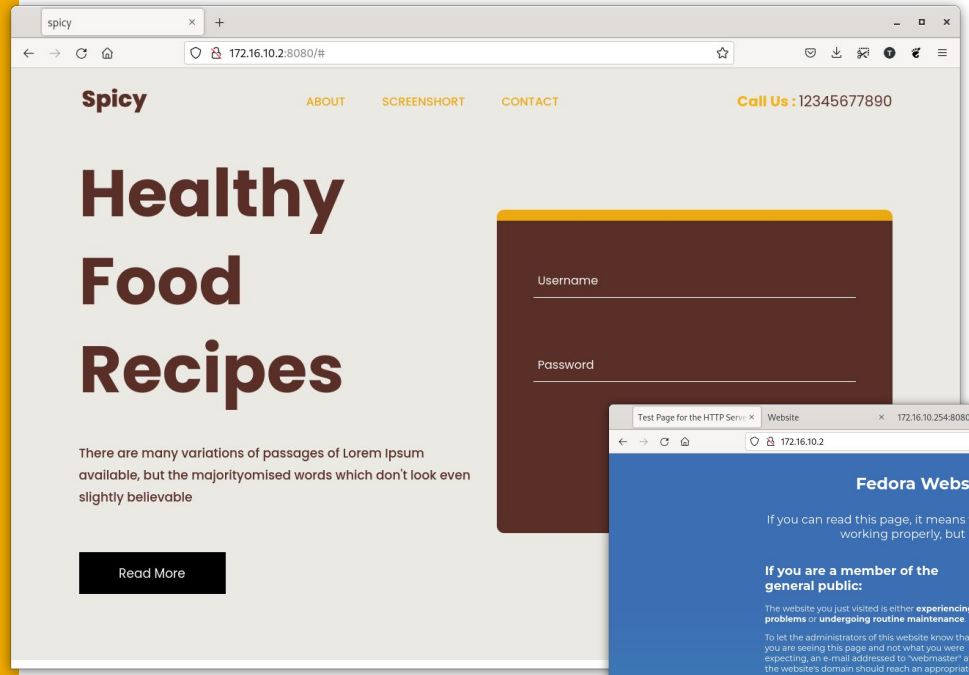
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Naše experimentální síť

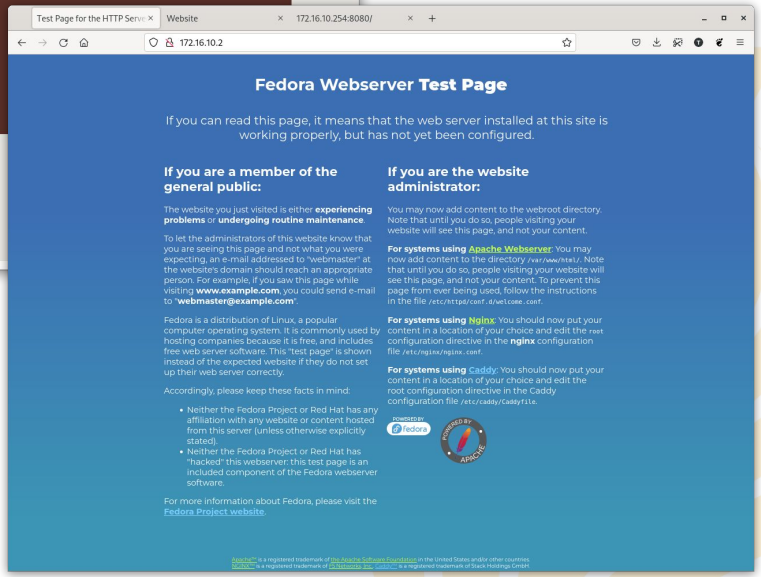


FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Naše experimentální síť



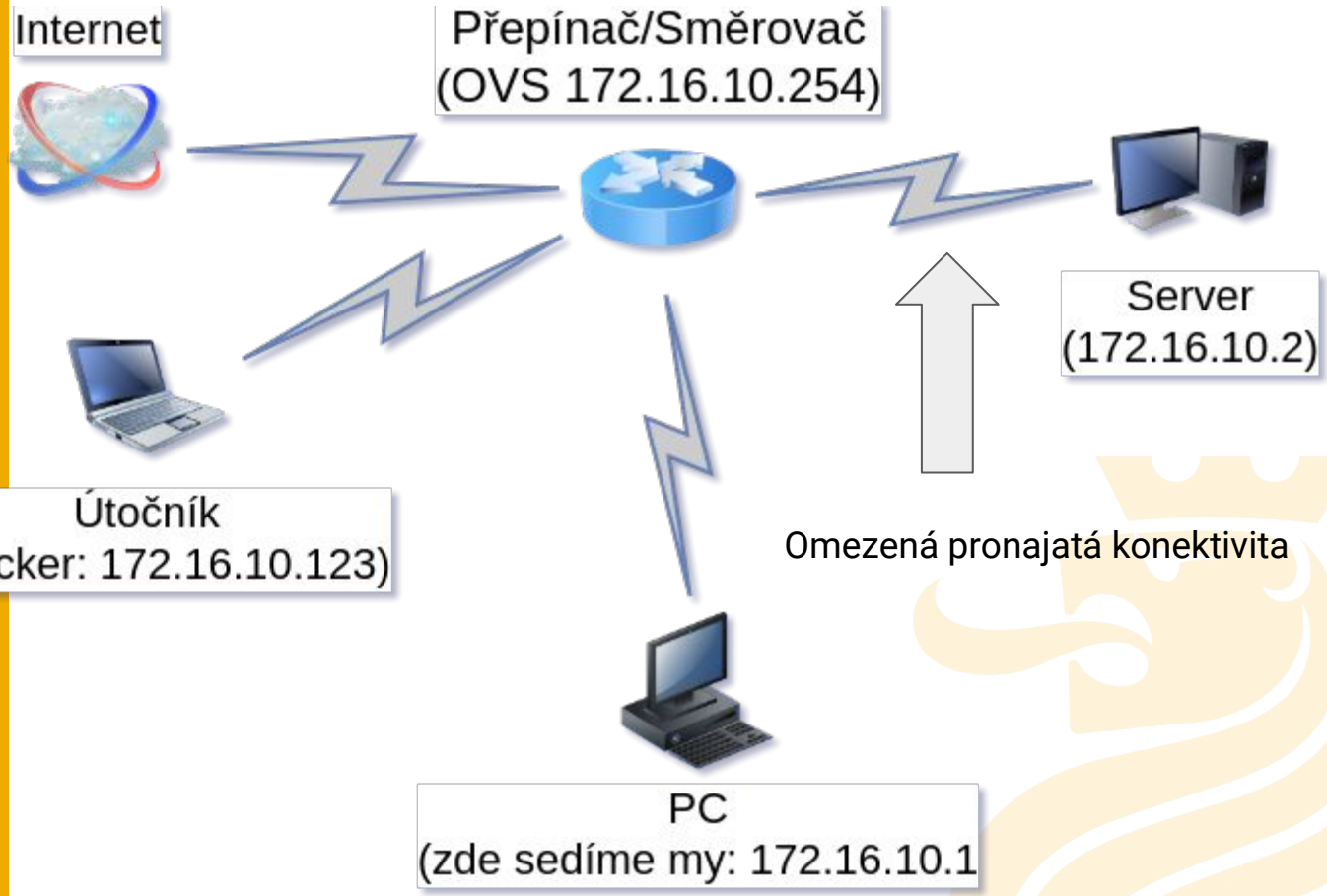
Server (172.16.10.2)




```
vagrant ssh server
```

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

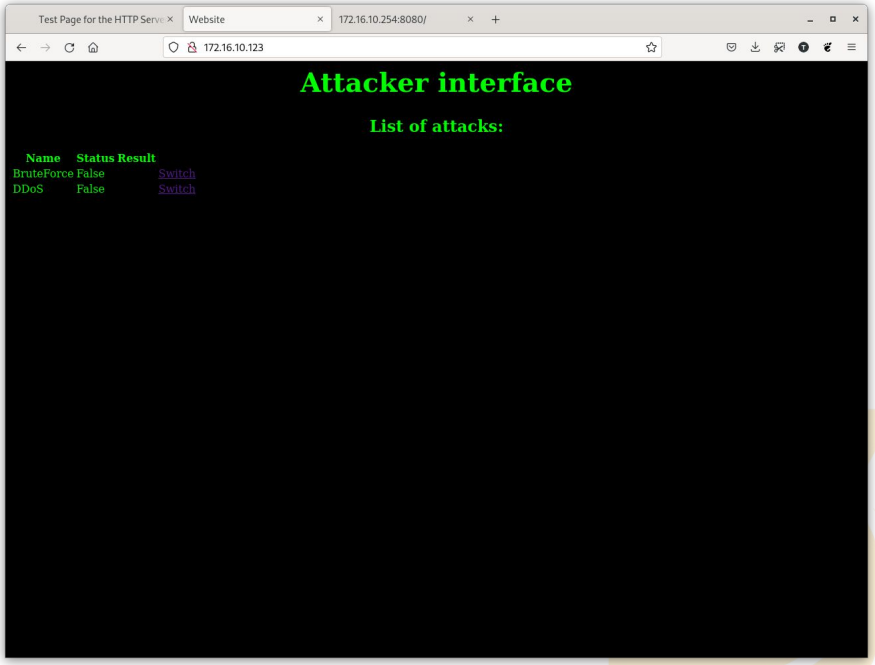
Naše experimentální síť



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

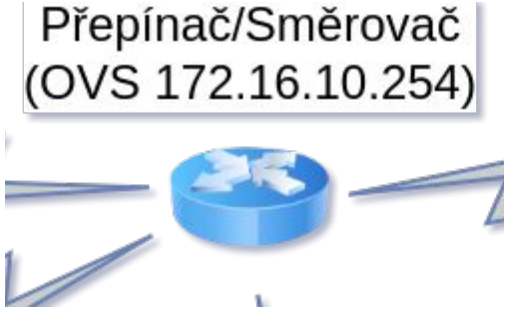
Naše experimentální síť

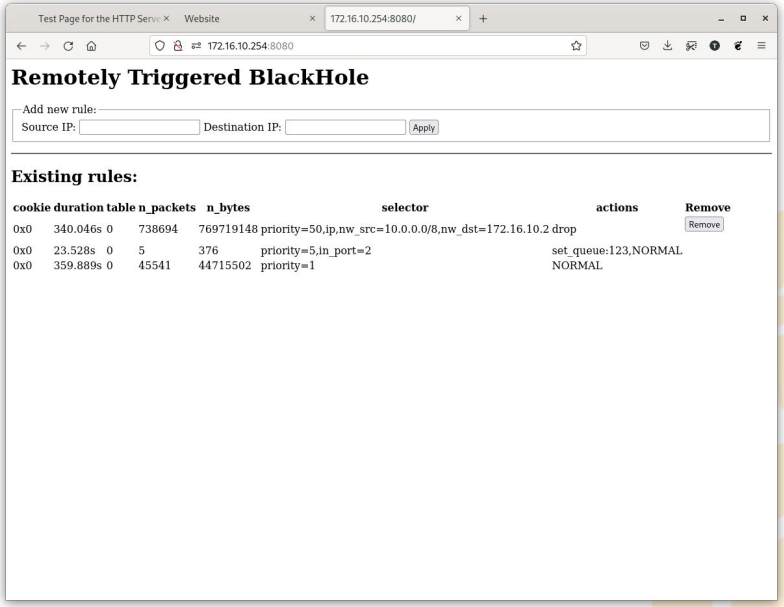
Útočník
(Attacker: 172.16.10.123)



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Naše experimentální síť





FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Úkol č.1 - jak se dostat na náš web server?

- V prohlížeči se nám nedaří otevřít testovací “stránku” http://172.16.10.2/
- Firewall na serveru blokuje provoz, který není povolen
- Zkusme povolit “port” web serveru:
  ```
  sudo firewall-cmd --add-service http
  ```
- Nyní již funguje! Ve firewallu serveru jsme povolili příchozí provoz odkudkoliv

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Úkol č.2 - Útočník hádá hesla do naší webové aplikace!!!

- Máme na webu přihlašovací formulář http://172.16.10.2:8080/login
- (útočníka spustíme my… ;-) pomocí http://172.16.10.123/ -> BruteForce)
  - Na Serveru vidíme události v logu pomocí:
    ```
    sudo journalctl -f -u webapp
    ```
- Co s tím?!
  - Opět můžeme zkusit firewall na našem serveru
- Můžeme zkusit na našem serveru zablokovat přímo útočníka:
  ```
  sudo firewall-cmd --zone=drop
      --add-source 172.16.10.123
  ```

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Úkol č.3 - Útočník zahlcuje linku k našemu serveru :’(

- (útočníka opět spustíme my, pomocí http://172.16.10.123/ -> DDoS)
- Co s tím?!
  - Při zahlcení linky už nám nepomůže zahazovat provoz až u nás…
- V takovém případě možná pomůže poskytovatel konektivity!
- Remotely Triggered Black Hole (RTBH):
  - Partnerská síť, přes kterou přichází útok, nám může pomoci filtrovat již po cestě.
  - Tzn. vzdáleně nastavíme zahazování paketů útočníka, které se ani nedostanou k našemu serveru.
- http://172.16.10.254:8080/
- Na Serveru dokážeme pozorovat příchozí pakety:

```
sudo tcpdump -nnn -i eth1
```

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Ing. Tomáš Čejka, Ph.D.

E-mail: cejkato2@fit.cvut.cz, cejkat@cesnet.cz
Twitter: @tomcejka
Laboratoř monitorování síťového provozu, FIT ČVUT v Praze
https://netmon.fit.cvut.cz