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

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Nežádoucí komunikace :-(

- Cizí “uživatel” se snaží přihlásit
  (útok hrubou silou, hádání přihlašovacích údajů, “brute-force”)
- Záludný “uživatel” pošle nebezpečný obsah
  (pokus o zneužití zranitelnosti aplikace, která nedokáže správně zpracovat vstup, “vulnerability exploit”)
- Někdo víc než dokážeme přijmout
  (naše připojení má omezenou kapacitu, ale přes poskytovatele přichází mnohem víc… “Distributed Denial of Service” - DDoS)

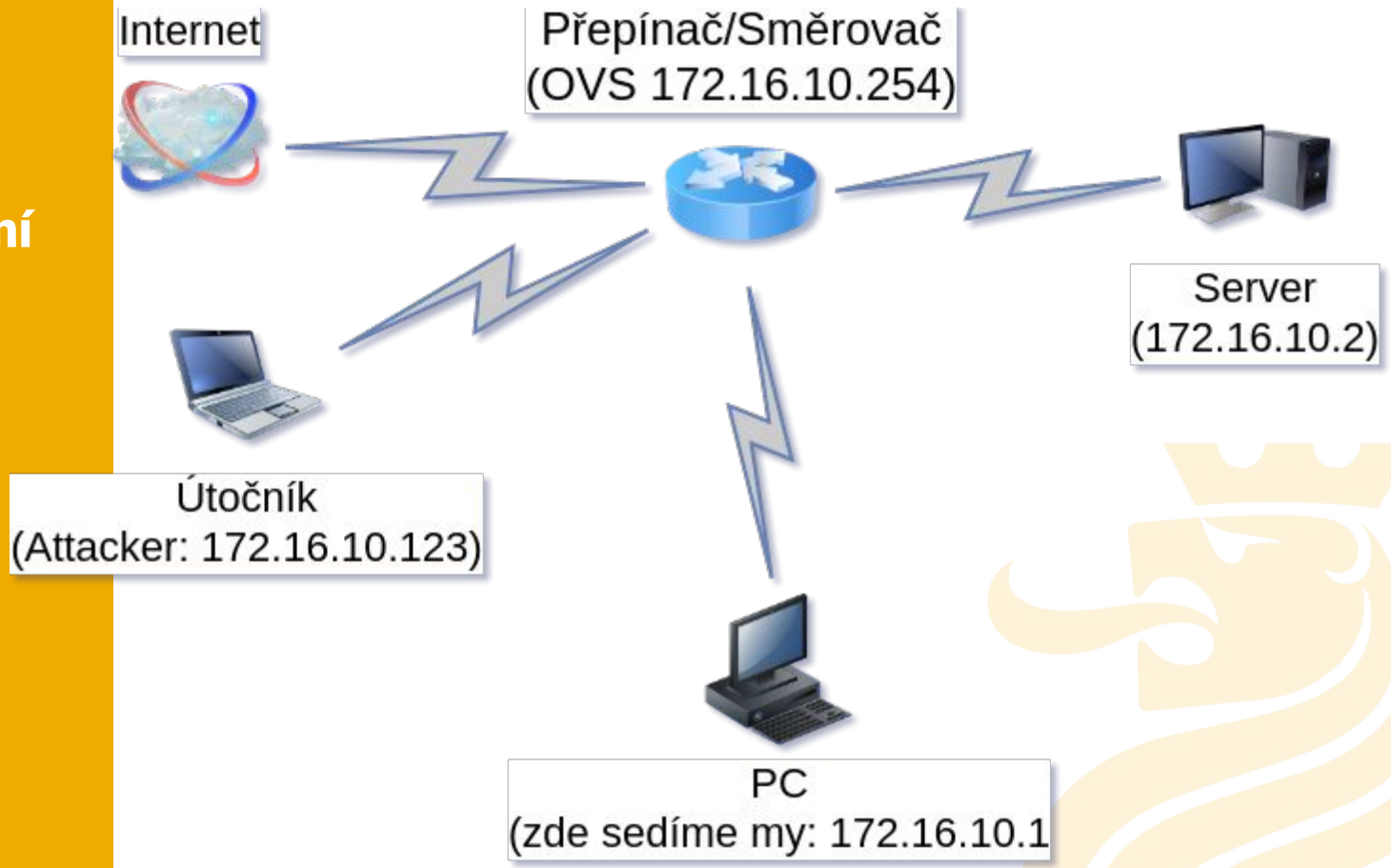
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

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

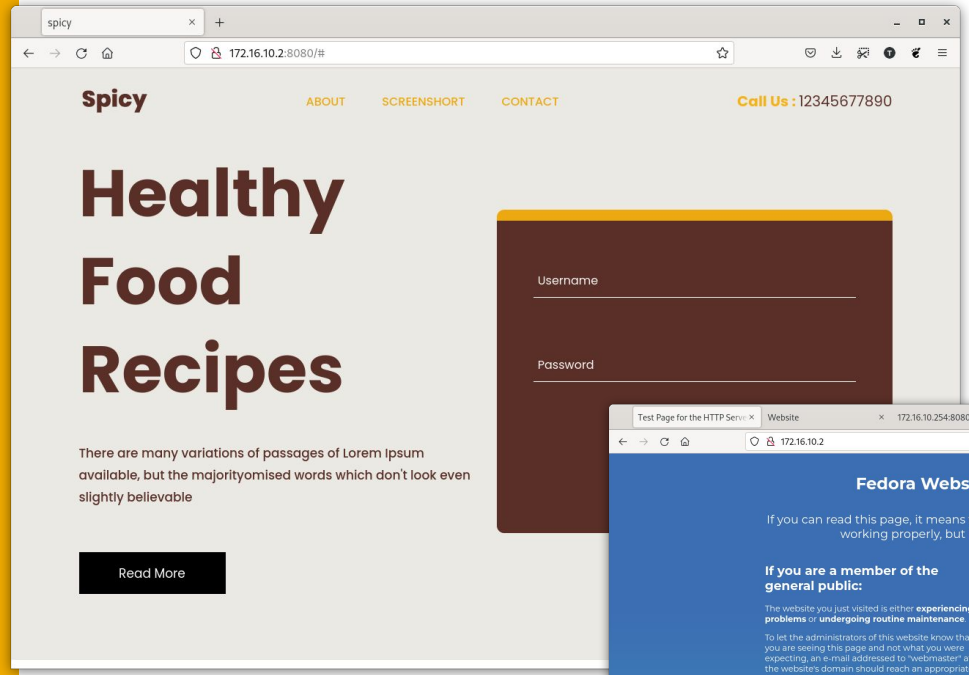
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Naše experimentální síť

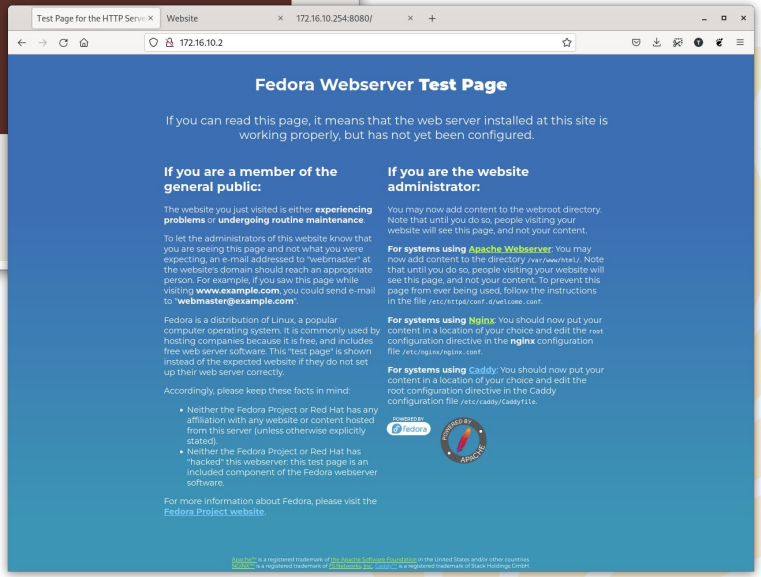


FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Naše experimentální síť



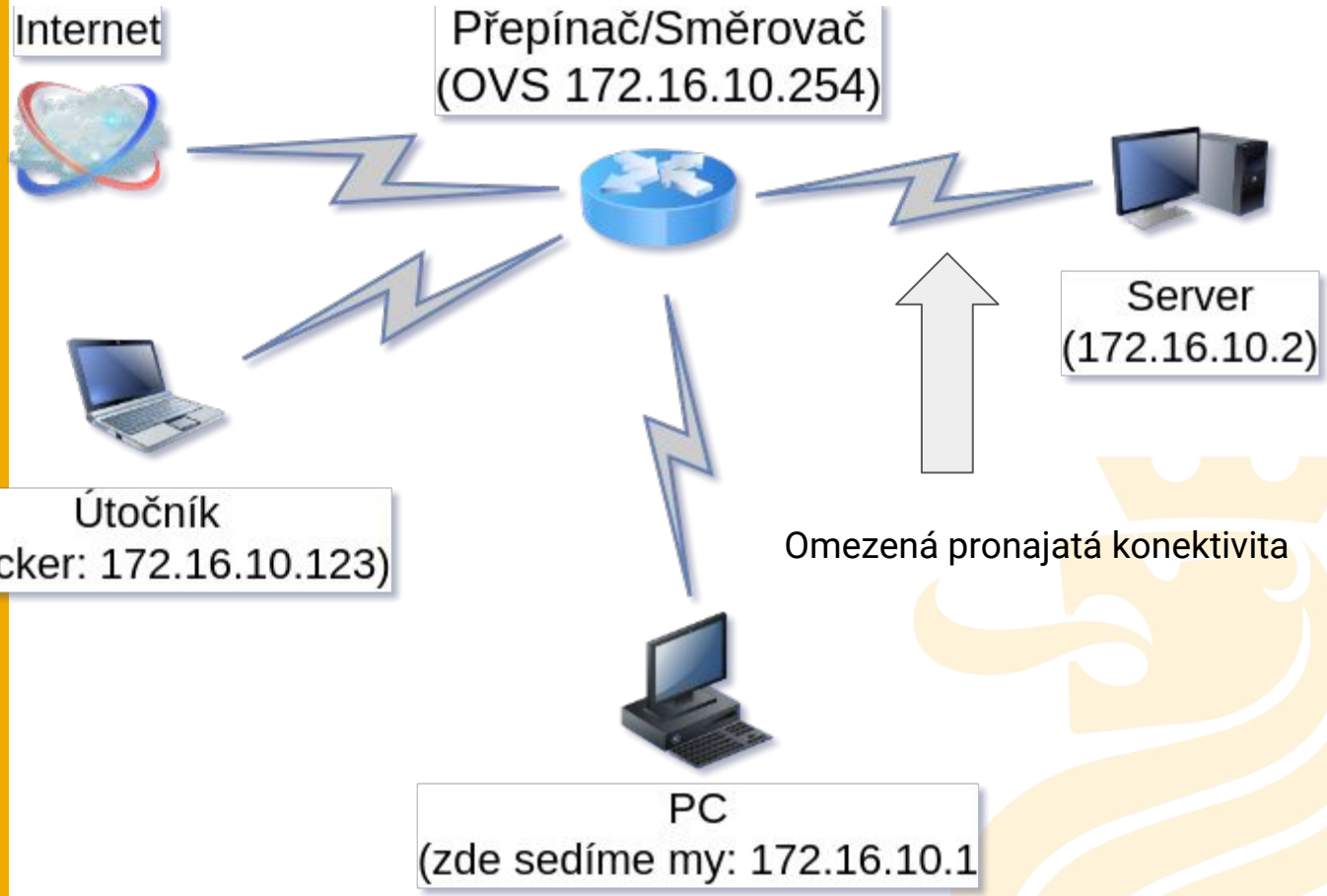
Server (172.16.10.2)




```
vagrant ssh server
```

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

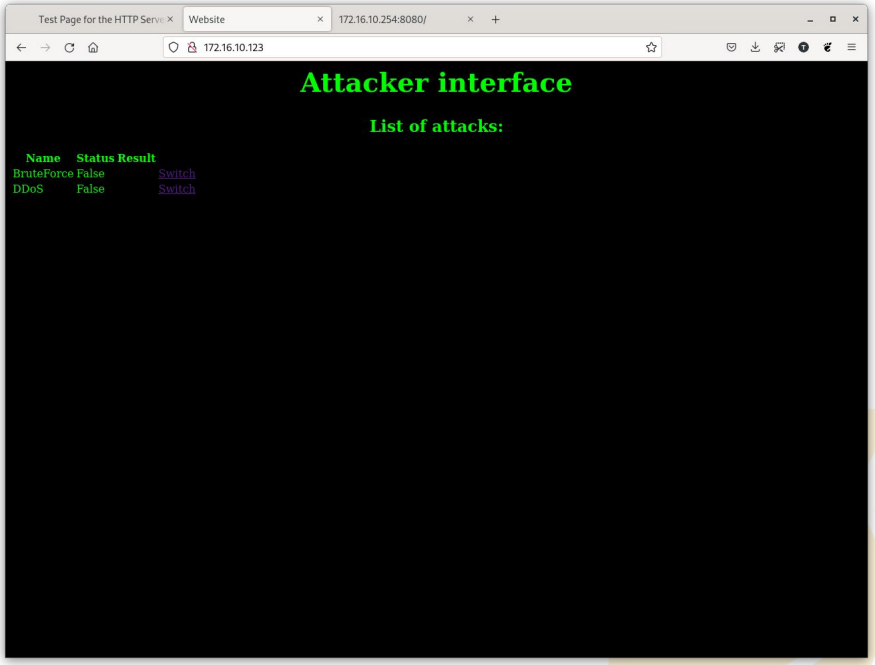
Naše experimentální síť



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

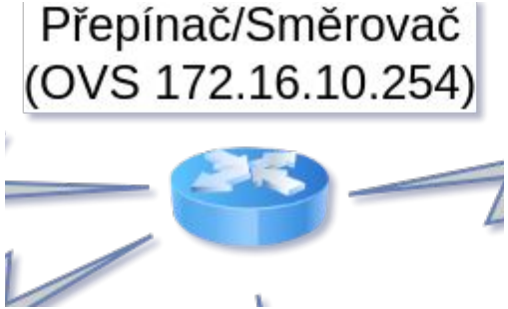
Naše experimentální síť

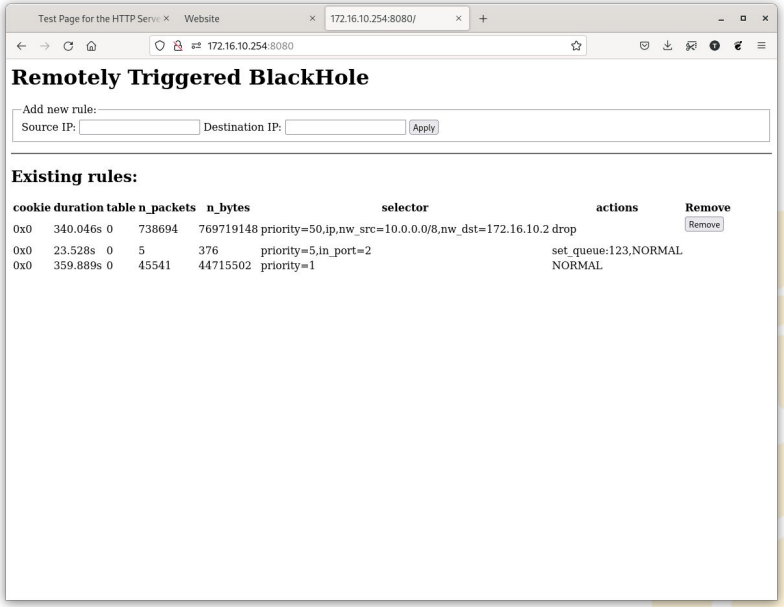
Útočník
(Attacker: 172.16.10.123)



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
```