



# Etické hackování a penetrační testy

Diplomová práce



Vojtěch Kessler

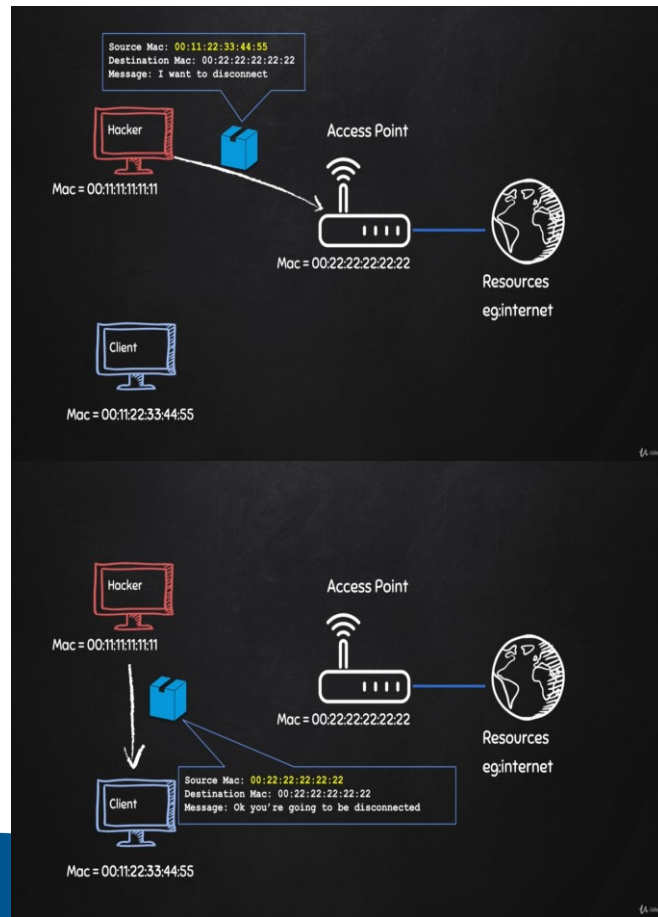
# Cíl práce

- analyzovat metody, které ohrožují počítačový systém
  - syntéza
  - komparace
- ochrana obchodu i jeho zákazníků
- relevantní metody => demonstrovány na virtuálním stroji => návrh způsobů ochrany
  - pozorování
  - komentování



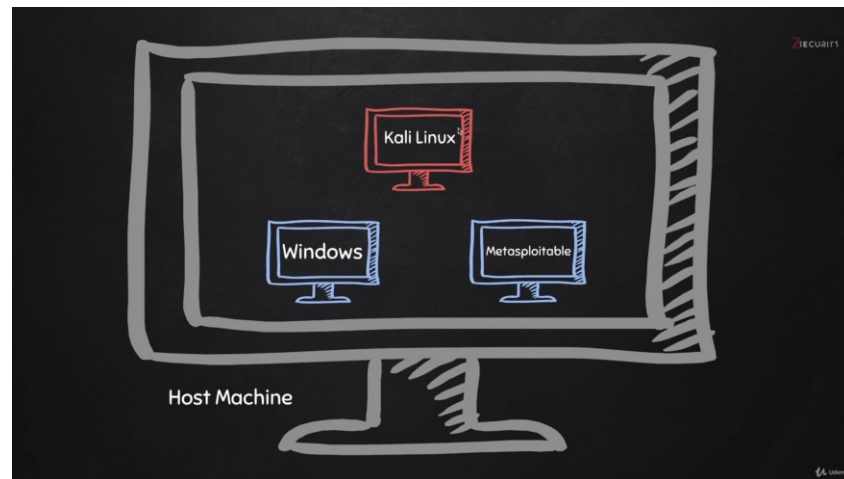
# Metodika – teoretická část

- metody hackování – server side + client side
- website hacking
- výběr nástrojů na hledání zranitelností => ochrana proti nejběžnějším útokům
- použita odborná literatura



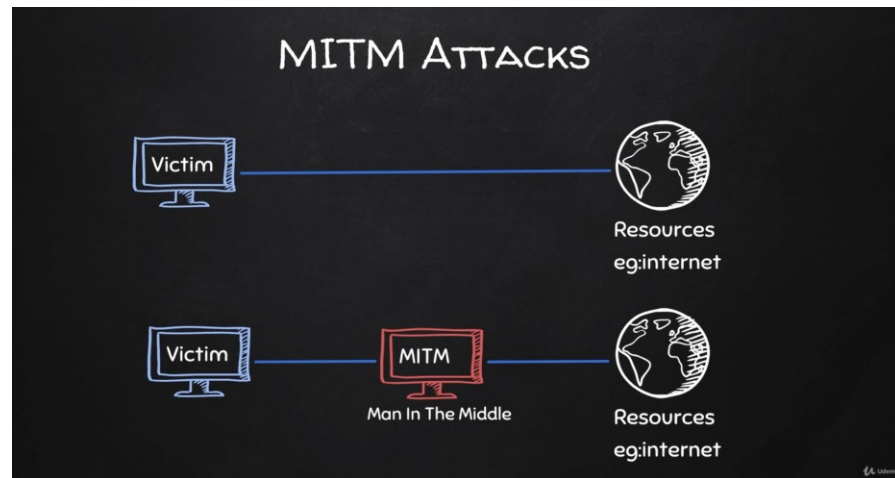
# Metodika – praktická část

- demonstrovány nejrelevantnější typy útoků pro e-shop
- virtuální stroj
- attacking-machine(kali-linux)
- client-machine (Metasploitable - linux s připravenými zranitelnostmi, Windows 10 with Legacy Microsoft Edge and Internet Explorer 11)
- netestováno na reálném webu, neboť to neumožňuje zákon bez písemného souhlasu, byť by šlo jen o monitorovací nástroj (40/2009 Sb. Trestní zákoník § 230, § 231 § 232)



# Výsledky praktické části práce

- WPA2 – dostatečně silné heslo, vypnutí funkce WPS
- detekce změn v ARP tabulce
- Wireshark – detekce podezřelých aktivit
- HTTPS Everywhere – detekce Man-in-the-Middle
- VPN a Proxy
- kontrola typu souborů
- allowed list a denied list, filtry
- přidělení jen nutných práv



# Závěr

- fyzický útok
- BSD



HTTPS Everywhere si všimlo přechodu na stránku bez HTTPS a pokusilo se zaslat namísto toho HTTPS verzi. Verze s HTTPS je nedostupná. Tato stránka pravděpodobně HTTPS nepodporuje nebo verzi HTTPS blokuje útočník. Pokud chcete zobrazit nešifrovanou verzi této stránky, vypněte v nastavení rozšíření HTTPS Everywhere volbu „Šifrované připojení ke všem serverům, kde je dostupné“. Mějte prosím na paměti, že vypnutím bude váš prohlížeč zranitelný vůči síťovým degradačním útokům na stránkách, které navštívíte.

[síťový degradační útok](#)

URL: <http://pocasi.siliconhill.cz/weather/>

Otevírat nezabezpečené stránky

Otevřít nezabezpečenou stránku (jen v této relaci)