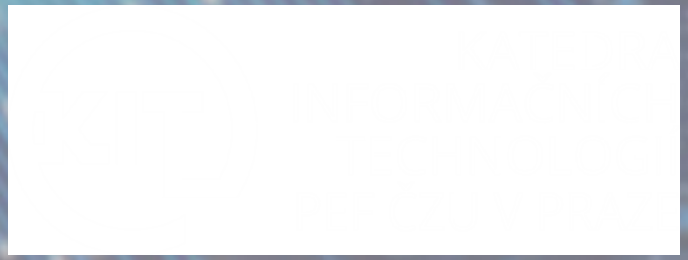


Etické hackování a penetrační testy

Diplomová práce

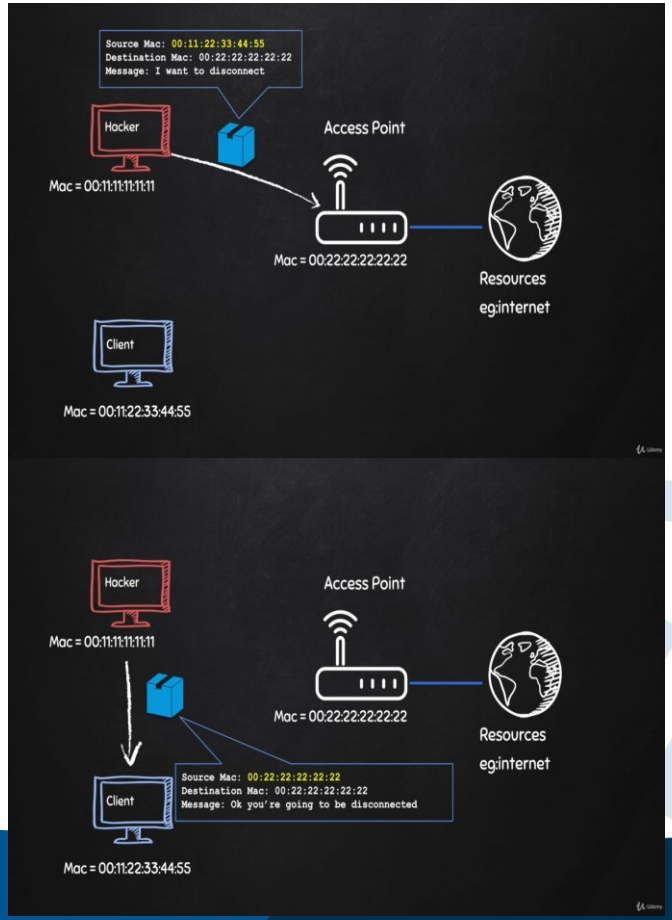
Vojtěch Kessler

Cíl práce

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

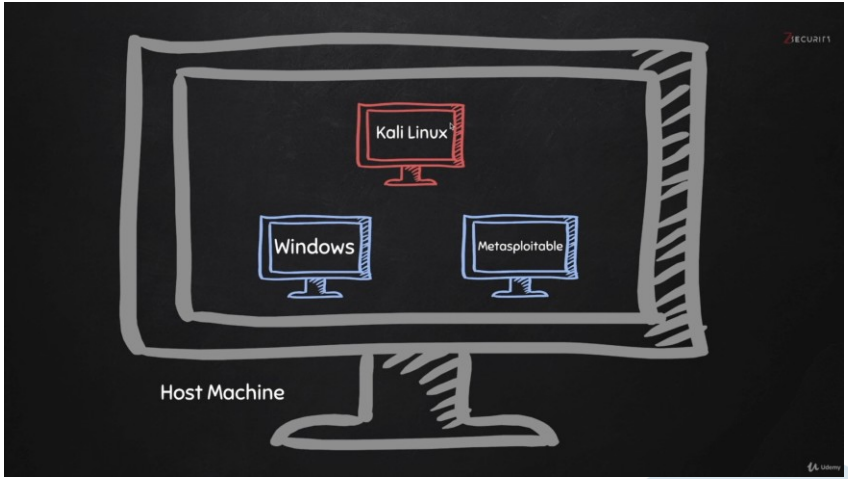
Metodika – teoretická část

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



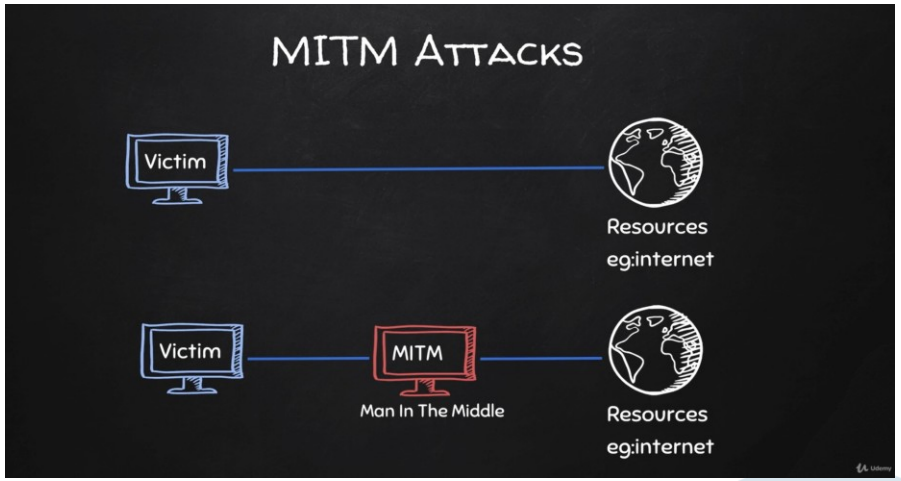
Metodika – praktická část

- 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