

ETICKÉ HACKERSTVO

Bakalárska práca sa zaoberá problematikou etického hackovania a úvodu do sveta informačnej bezpečnosti. Práca je rozdelená do troch hlavných častí. V prvej časti je objasnený termín hacker a ako ich podľa zámeru rozdeľujeme do skupín na takzvané farby klobúkov. Ďalšie rozdelenie je podľa ich špecifikácie a skúseností. Zdôrazňuje sa fakt, že hackeri nie sú len tí čo konajú protizákonne, ale aj tí čo sa snažia chrániť systém. Práca sa zaoberá hlavne etickými hackermi, ktorých práca je vykonávať penetračné testy. V druhej časti sú teoreticky opísané dôvody a ciele spracovania tejto problematiky. Sú vysvetlené rôzne druhy penetračných testov a taktiež rozdelenie testovania na určité fázy a metódy, ktoré sú použité v nich. Sú predstavené nástroje, ktorými môžeme automatizovať útok na systém. V tejto časti sú prakticky spracované ukážky, pri ktorých je opísaný presný postup ako som pracoval a vysvetlenie toho postupu. Použité príkazy sú vysvetlené tak aby tomu rozumel aj človek, ktorý sa nezaoberá informatikou. Ďalej chcem ukázať čitateľom, s akými metódami pracujú hackeri a tým naznačiť čomu by sa mali vyhnúť, ako sa lepšie chrániť a nenechať sa oklamať. V poslednej časti som vyjadril svoj názor, prečo by bolo dobré zaradiť túto problematiku do vyučovacieho procesu. Takisto prečo by sme mali dbať na bezpečnosť technológií.

Kľúčové slová: informačná bezpečnosť, etické hackerstvo, penetračný test

Autor: Filip Boháč

Vedúci bakalárskej práce: Mgr. Jozef Siláči



```
root@kali:~# nmap -sS -p- 10.0.2.4 -v -T4

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-28 11:57 EST
Initiating ARP Ping Scan at 11:57
Scanning 10.0.2.4 [1 port]
Completed ARP Ping Scan at 11:57, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:57
Completed Parallel DNS resolution of 1 host. at 11:57, 0.04s elapsed
Initiating SYN Stealth Scan at 11:57
Scanning 10.0.2.4 [65535 ports]
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 5900/tcp on 10.0.2.4
Discovered open port 3306/tcp on 10.0.2.4
Discovered open port 139/tcp on 10.0.2.4
Discovered open port 445/tcp on 10.0.2.4
Discovered open port 111/tcp on 10.0.2.4
Discovered open port 21/tcp on 10.0.2.4
Discovered open port 25/tcp on 10.0.2.4
Discovered open port 22/tcp on 10.0.2.4
Discovered open port 53/tcp on 10.0.2.4
Discovered open port 23/tcp on 10.0.2.4
Discovered open port 36930/tcp on 10.0.2.4
Discovered open port 1099/tcp on 10.0.2.4
```



```
root@kali:~# sqlmap
```



The logo features a central vertical red bar with a yellow 'H' at the top and a yellow 'V' at the bottom. To the left of the bar is a yellow bracket containing a yellow 'C'. To the right of the bar is a yellow bracket containing a yellow '1'. The background is black with yellow lines forming a grid-like pattern.

{1.1.12#stable}

<http://sqlmap.org>

```
Usage: python sqlmap [options]
```