Student name: Joel Mäenpää

Class (if Oamk/Ouas student): DIN18SP

Email address (prefer you @students.oamk.fi email): t8majo03@students.oamk.fi

# Week 1 – Introduction

Question 1: What is nmap?

Answer 1: Nmap [1] is a security testing tool to actively scan (enumerate) IP networks and services. Nmap has a modular scripting engine and it can be used to improve basic scanning features. For example, locating unpatched Samba installations vulnerable to CVE-2017-7494 [2].

[1] <https://nmap.org/>

[2] <https://nmap.org/nsedoc/scripts/smb-vuln-cve-2017-7494.html>

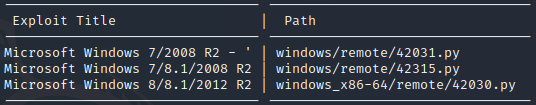
Question 2: Scan host www.teemukorpela.fi with Kali's nmap basic scan. Which TCP-ports are open?

Answer 2: Just the ports 80 and 443, so HTTP and HTTPS according to nmap.



Question 3: Use Kali's "searchsploit"-command to list all EternalBlue exploits available. How many were there? What is EternalBlue vulnerability?

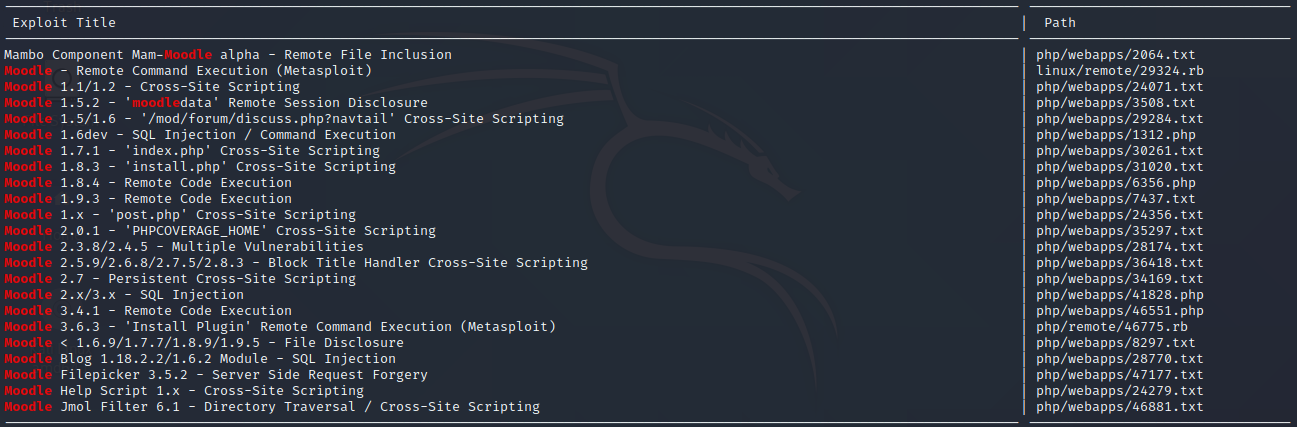
Answer 3: 3 exploits available. EternalBlue [1] exploits a vulnerability in Microsoft’s implementation of the Server Message Block protocol, which is a network file sharing protocol allowing access to files on remote servers.



[1] <https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf>

Question 4: Search Moodle vulnerabilities with Kali's searchsploit and Google

Answer: Exploits from searchsploit:



Snyk.io [1] lists multiple other vulnerabilities like cross-site scripting, denial of service, and authentication bypassing.

[1] <https://snyk.io/vuln/composer:moodle%2Fmoodle>

Question 5: What is "security through obscurity"?

Answer 5: Security through obscurity [1] means securing a system by hiding the system’s security flaws through secrecy and confidentiality.

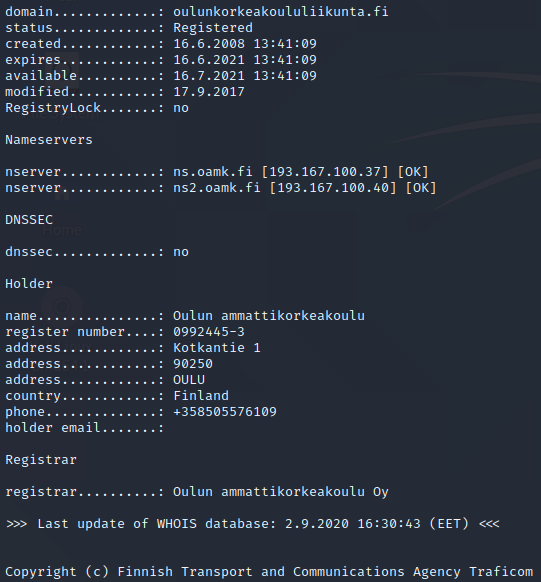
[1] <https://www.techopedia.com/definition/21985/security-through-obscurity-sto>

Question 6: What kind of information security problems and vulnerabilties automated vulnerability scanners (Nessus, OpenVAS and such) cannot usually detect?

Answer 6: Vulnerabilities that might arise from the end-users actions, such as keeping their system up to date and in general staying safe.

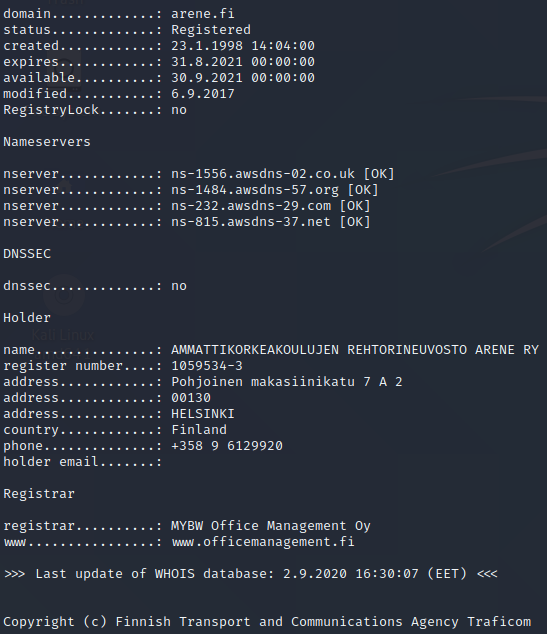
Question 7: Resolve who is the owner / has registered domain oulunkorkeakoululiikunta.fi?

Answer 7: Oulun ammattikorkeakoulu



Question 8: Resolve who is the owner / has registered domain arene.fi?

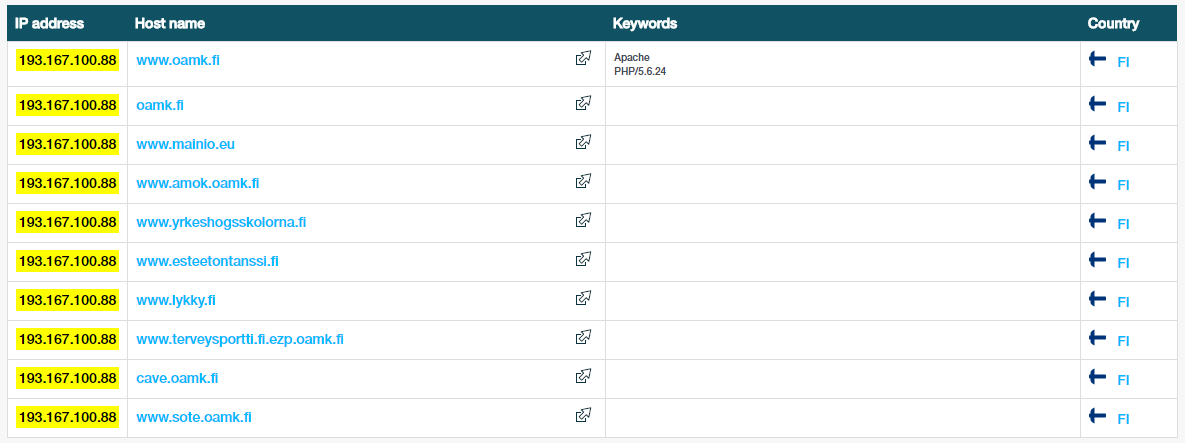
Answer 8: Ammattikorkeakoulujen rehtorineuvosto arene ry



Question 9: Use Internet Archive's Wayback Machine to solve who was the director of research and development in Oamk in March 2012? (http://www.oamk.fi/english/ouas/rd/)

Answer 9: Irene Isohanni

Question 10: Use riddler.io, robtex.com or securitytrails.com to resolve what virtual web servers have been hosted in 193.167.100.88

Answer 10: 

Question 11: Locate OVH.com (ovh-group) corporation from Hackerone.com's bounty program: What hosts/services are currently in the limited scope allowed to the hacked/tested?

Answer 11: Currently the program is limited to vulnerabilities found in OVH’s [1] main API

[1] <https://hackerone.com/ovh-group>

Question 12: Register to Shodan.io and study how many internet visible MySQL services are in Sweden according to Shodan?

Answer 12: 3520 [1]



[1] <https://www.shodan.io/search?query=mysql+port%3A%223306%22>

Question 13: Explanations

Answer 13:

* White hat, black hat — The difference between white hat and black hat [1] hacking is that white hats are ethical hackers and black hats are “criminal” hackers.
* CVE / CVSS — CVE [2] is a list of publicly disclosed vulnerabilities. CVSS [2] is a scoring system used in vulnerability management programs.
* Proof-of-concept — Proof-of-concept [3] is an exercise where you determine if an idea can be turned into reality.
* Zero day attack / vulnerability — Zero day attack [4] is an attack that exploits a software security weakness that the developer may be unaware of.
* Script kiddie — Script kiddie [5] is a person who is using scripts already written to hack into computers, for the lack of ability to write their own
* Social engineering — Social engineering [6] is basically manipulation to make people give up confidential information.
* Spear phishing — Spear phishing [7] is the practice of sending fake emails from trusted sender in order to get the target to reveal confidential information.
* Port scanning — Port scanning [8] is a method to probe a server or a host to determine which ports are open and could be receiving or sending data.
* Shodan and Censys — Shodan [9] is a search engine for Internet-connected devices that gathers information about all devices connected the the Internet. Censys [10] is a platform which helps information security practitioners discover, monitor, and analyze devices accessible to the Internet.
* Kali Linux — Kali Linux [11] is a Debian-based Linux distro which is used for security audition and penetration testing.
* Metasploit — Metasploit [12] is an exploitation and vulnerability validation tool that helps you divide the penetration testing workflow into manageable sections.

[1] <https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html>

[2] <https://www.balbix.com/insights/whats-the-difference-between-cve-and-cvss/>

[3] <https://searchcio.techtarget.com/definition/proof-of-concept-POC>

[4] <https://www.investopedia.com/terms/z/zero-day-attack.asp#:~:text=A%20zero%2Dday%20attack%20(also,the%20threat%20to%20software%20users.>

[5] <https://www.uscybersecurity.net/script-kiddie/>

[6] <https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering>

[7] <https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing>

[8] <https://www.avast.com/business/resources/what-is-port-scanning#:~:text=Port%20scanning%20is%20a%20method,analyzing%20responses%20to%20identify%20vulnerabilities.>

[9] <https://help.shodan.io/the-basics/what-is-shodan>

[10] <https://about.censys.io/>

[11] <https://www.kali.org/docs/introduction/what-is-kali-linux/>

[12] <https://docs.rapid7.com/metasploit/>

# Week 2 – Nnnn

Question 1: Nnnn

Answer 1: Nnnnn

Question 2: Nnnn

Answer 2: Nnnnn

…

…

# Week 3 – Nnnn

Question 1: Nnnn

Answer 1: Nnnnn

Question 2: Nnnn

Answer 2: Nnnnn

…

…

# Week 4 – Nnnn

Question 1: Nnnn

Answer 1: Nnnnn

Question 2: Nnnn

Answer 2: Nnnnn

…

…

# Week 5 – Nnnn

Question 1: Nnnn

Answer 1: Nnnnn

Question 2: Nnnn

Answer 2: Nnnnn

…

…

# Week 6 – Nnnn

Question 1: Nnnn

Answer 1: Nnnnn

Question 2: Nnnn

Answer 2: Nnnnn

…

…

# Week 7 – Nnnn

Question 1: Nnnn

Answer 1: Nnnnn

Question 2: Nnnn

Answer 2: Nnnnn

…

…