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>

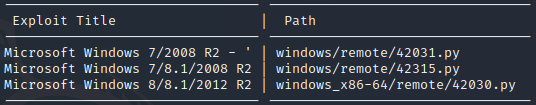
Question 2: Scan host www.teemukorpela.fi with Kali's nmap basic scan. Which TCP-ports are open?

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?

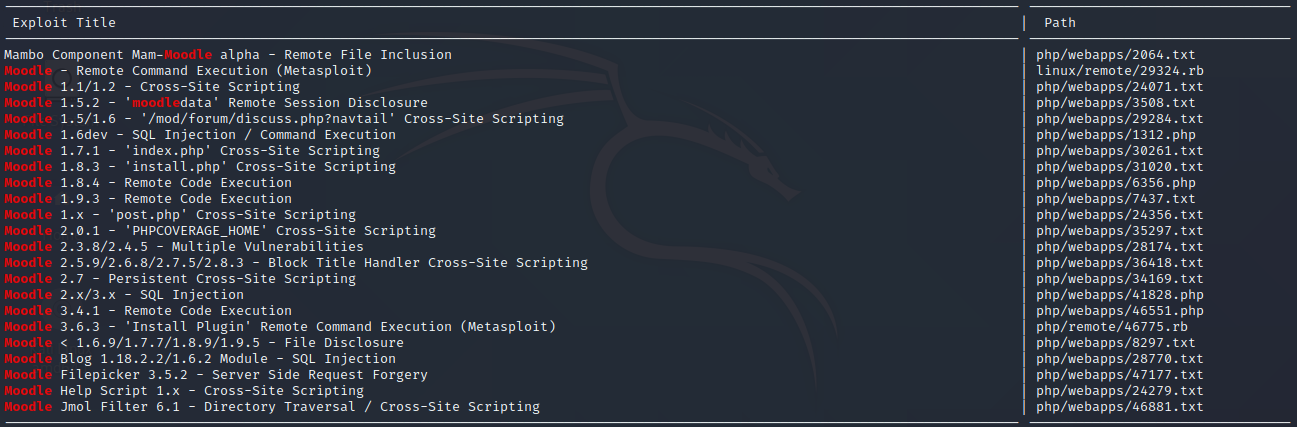
Answer 3: 3 exploits available. EternalBlue [1] exploits a vulnerability in Microsoft’s implementation of the Server Message Block protocol, which is a network file sharing protocol allowing access to files on remote servers.



[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.

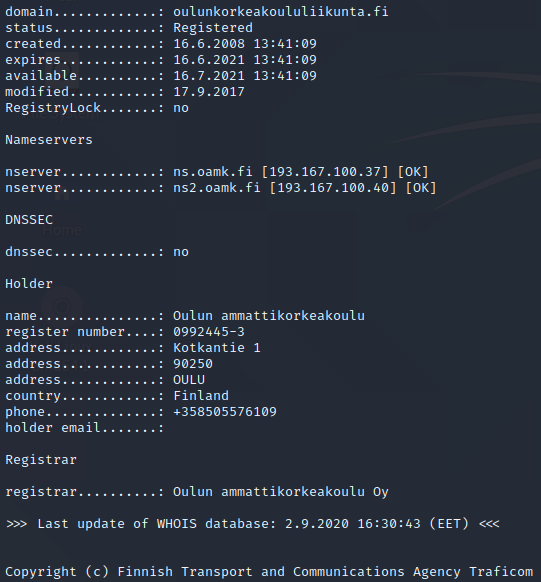
[1] <https://www.techopedia.com/definition/21985/security-through-obscurity-sto>

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.

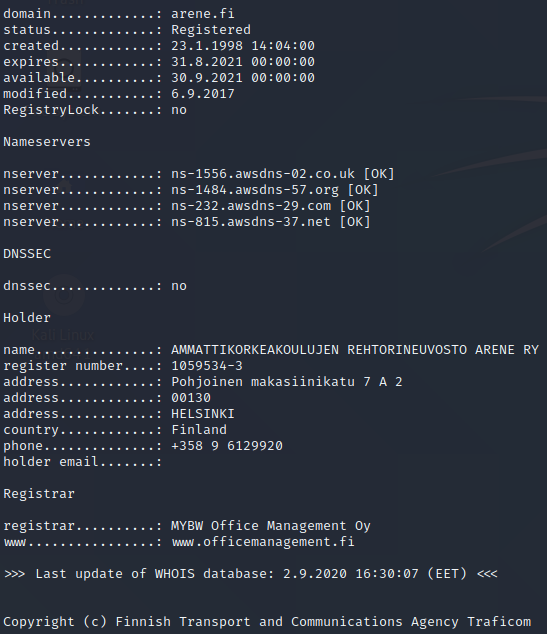
Question 7: Resolve who is the owner / has registered domain oulunkorkeakoululiikunta.fi?

Answer 7: Oulun ammattikorkeakoulu



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

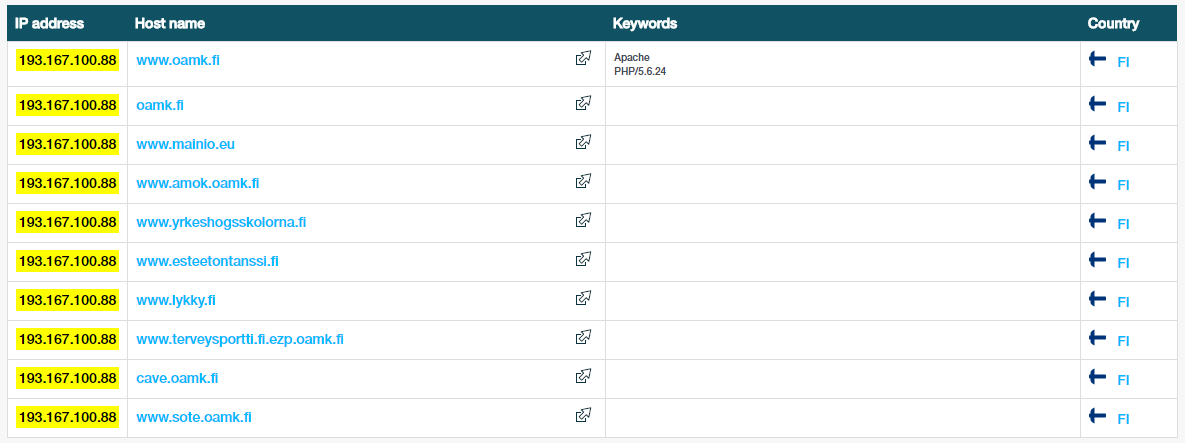
Answer 8: Ammattikorkeakoulujen rehtorineuvosto arene ry



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 – Software vulnerabilities

Question 1: Explain Microsoft's STRIDE threat model shortly.

Answer 1: Microsoft’s STRIDE [1] stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Spoofing means impersonating, tampering stands for modifying data or code, repudiation as in claiming not to have performed an action, information closure means letting unauthorized people see and use information, denial of service stands for denying access to a service, and elevation of privilege means gaining capabilities without proper authorization.

[1] <https://www.microsoft.com/security/blog/2007/09/11/stride-chart/>

Question 2: Explain Microsoft's DREAD risk model shortly.

Answer 2: Microsoft’s DREAD [1] stands for Damage, Reproducibility, Exploitability, Affected users, and Discoverability. Damage means to assess the damage that could result from an attack, reproducibility measures how often a specified type of attack will succeed, exploitability means to assess the amount of work and knowledge to mount an attack, affected users is the number of users affected by a potential attack, and discoverability is the possibility a threat will get exploited.

[1] <https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers>

Question 3: Study D-Link DNS-320 ShareCenter write-up in the ExploitDB. What kind of software exploit is that? Try to explain shortly how the attacker can elevate his/her access to a root shell?

Answer 3: A remote code execution exploit. Exploiting a hardcoded backdoor the hacker could logout with the “name” parameter set to malicious PHP code as the “name” parameter is never sanitized. Then the hacker can use cat to read the user log file and pipe it to a web directory and create a PHP web shell. Now the hacker can just use the web shell to execute any PHP code as root.

Question 4: Study CVE-2017-8759-Exploit-sample and estimate risks for enterprise networks: What kind of mitigations would fix/stop/prevent hostile code being executed by users who are being targeted by this attack?

Answer 4: Keeping your software and protections up to date is already a good way to prevent this type of attacks from happening. Staying vigilant and listening to experts in the field also betters the users chances of not getting attacked.

Question 5: Study CWE-208 weakness and CVE-2016-6210 vulnerability. Overall, how to prevent such attacks?

Answer 5: When preventing timing attacks [1] you should use proper cryptographic libraries and helper functions. Rate limiting or CAPTCHA also provides some protection against timing attacks but doesn’t necessarily solve the problem.

[1] <https://stackoverflow.com/questions/47743761/main-techniques-for-preventing-timing-attacks>

Question 6: Read the blog post "I’m harvesting credit card numbers and passwords from your site. Here’s how". What can you do to improve the security of software supply chain?

Answer 6: Well, according to the blog post, moving to a secluded cabin in the middle of a forest with a lake (or a river) right next to it is a plausible solution. The blog post also gives a second option for safety. When creating pages for login, register, and credit card collection, using your own lightweight pages with your own JavaScript is the way to go. Having a ton of npm packages in these pages could prove fatal to the service being created.

Obviously the blog post is made in a sarcastic fear mongering sense, but knowing what packages, libraries, and frameworks you use is important when creating services that make use of people’s personal information.

I could not answer the hacking questions, because of the broken linux server not being able to connect to Internet using NAT.

# Week 3 – Common web attacks and very basics of cryptography

Question 1: Describe shortly these web vulnerabilities:

* Injection (for example SQLi) – Code injection technique, used to attack data-driven applications.
* Insecure Deserialization (for example handling cookie data) – A vulnerability which occurs when untrusted data is used to abuse the logic of an application.

Question 2: Describe shortly following web security tools/terms/concepts:

* Let's encrypt – A free, automated, and open certificate authority.
* HSTS – A web security policy mechanism that helps protect websites against man-in-the-middle attacks.
* WAF – A specific type of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service.
* Netsparker – A platform for all kinds of we application security needs.

Question 3: Describe shortly following information security terms/concepts:

* Plain text protocol – A protocol where the content is in human-readable form.
* Dictionary attack – A brute force method of breaking into a password-protected computer or server by systematically entering words in a dictionary as password.
* Rainbow table – A precomputed table used for caching the output of cryptographic hash functions.
* Steganography – A technique of hiding secret data within another file.
* Code obfuscation – A deliberate act of creating source or machine code that is difficult for humans to read.
* Self-signed certificate – A certificate not signed by a certificate authority.
* PRNG – A pseudorandom number generator. Difference to TRNG (true random number generator) is that PRNGs use mathematical algorithms to generate random numbers and can be predicted.
* AES – A specification for the encryption of electronic data.

Question 4: This is a hashed password (SHA512). Crack it with any online cracker, or with John the Ripper or Hashcat. You should probably use this Finnish dictionary

Answer 4: hiippailija

# Week 4 – Networking

Question 1: Why DNS is so critical service for both locally and in the Internet (information security reasons)?

Answer 1: DNS links the domain name to the IP. Faking DNS records can potentially trick users into visiting fake websites and downloading malicious software.

<https://teamarin.net/2017/06/23/why-does-dns-security-matter/>

Question 2: Why source IP address spoofing is so easy in the Internet for (amplified) DDOS attacks?

Answer 2: Because the Internet global routing is based on the destination IP address.

<https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf>

Question 3: What is SYN flood and how SYN cookies will address/mitigate the attack?

Answer 3: A form of DoS attack [1] where the attacker sends SYN requests repeatedly to the target’s system. SYN cookies [2] mitigate attacks by calculating a specific TCP sequence number with a secret math function in the SYN-ACK response. When the server receives the ACK response from the client, the TCP sequence number gets checked against the function to determine if it’s a legitimate reply.

[1] <https://www.imperva.com/learn/ddos/syn-flood/>

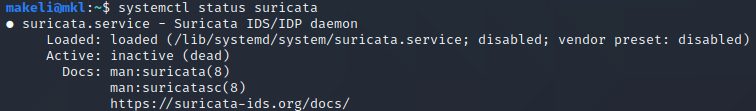
[2] <https://etherealmind.com/tcp-syn-cookies-ddos-defence/>

Question 4: Describe shortly following security tools/terms/concepts:

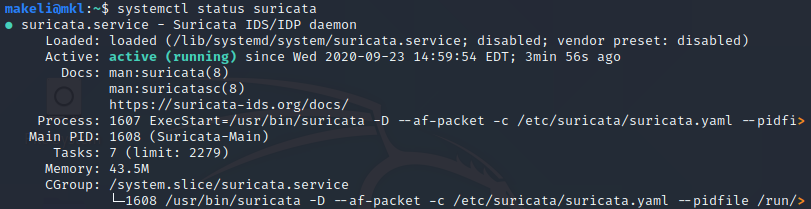
Answer 4:

* IPv6 privacy extension (RFC 4941) – It is a privacy extension for stateless address autoconfiguration in IPv6
* Rogue DHCP – A DHCP server which is not under the administration of the staff
* ARP spoofing – A type of attack where falsified ARP messages are sent over local area network
* Slowloris attack – A type of DoS attack tool which allows an attacker to overwhelm the targeted server by opening and maintaining many simultaneous HTTP connections between the attacker and the target
* War driving – The act of searching for Wi-Fi networks from a vehicle
* MitM – Man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communications between two parties
* IPSec – A group of protocols which are used together to set up encrypted connections between devices
* Wifi Pineapple – A tool originally created to allow testing of vulnerabilities of networks
* "Karma" wifi attack – A hack where the hacker tricks the target into joining a Wi-Fi network under their control
* Tunneling protocol – A communications protocol that allows for the movement of data from one network to another
* Data diode – A hardware device that allows data travel only to one direction

Question 5: Install Suricata to Kali with "apt install suricata" and start the service with "systemctl start suricata". Verify that Suricata is running with "systemctl status suricata"

Answer 5: 

Question 6: Restart the Suricata with "systemctl restart suricata" and verify that it is still running with "systemctl status suricata"

Answer 6: 

# Week 5 – Exploiting and Testing

Question 1: Read this five part article series: Reverse Engineering a router and answer these questions:

* What is U-boot? – A universal boot loader
* What is Busybox? – A software suite that provides Unix utilities
* What is SPI analyzer? – A protocol analyzer which samples an SPI bus and decodes the electrical signals
* What is SquashFS? – A read-only file system for linux which compresses files or directories

Question 2: Read this article about cracking SIM cards. and answer these questions:

* What is "side-channel attack"? – An attack that monitors things such as electromagnetic emissions, power consumption, and heat generation
* How side-channel attack was used to crack SIM cards? – The university team tracked the power levels of the card, monitored the data traffic, and correlated the results with a SIM card reader and a PC

Question 3: Describe shortly following security tools/terms/concepts:

* Disassembler – Translates machine language into assembly language
* Shellcode – Small piece of code used when exploiting a software vulnerability
* ASLR – Address space layout randomization is a technique trying to prevent the exploitation of memory corruption vulnerabilities
* Data Execution Prevention (DEP) – A security feature to help prevent damage done by viruses and other threats
* NX bit protection – A technology used in CPUs which allows to mark each memory page as being allowed or disallowed
* Stack canary – A value placed on the stack which changes every time the program is started
* Polymorphic code – Code that uses a polymorphic engine to change its binary signature while keeping the original algorithm the same
* Overflow vulnerability – A vulnerability caused by the buffer overflow
* Race condition vulnerability – A vulnerability which occurs when a computing system is forced to perform two or more operations simultaneously
* RCE vulnerability – A vulnerability that can be exploited if user input is injected into a file or a string and executed by the programming language’s parser
* Privilege escalation exploit – An exploit where the hacker is able to gain elevated access to resources that are normally protected

# 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

…

…