TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Hyökkäävä kyberturvallisuus

kurssikuvaus

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

Course instructions

Grading

To pass the course, you must gain access and write an acceptable report on at least three target machines, and get a passing grade on the exam.

Please see the separate reporting guidelines for thorough requirements. You may be deducted ½ point for an incomplete report. For each report over three, you gain an additional grade.

You must pass the practical exam at the end of the course (date to be announced). You will get 0-1 grade bonus depending on your exam result (1-5).

You will get 0-1 grade bonus depending on the number of completed assignments. Scale:

70% – ½ grade (will show up in gradebook as 1)

90% – 1 grade (will show up in gradebook as 2)

Using TryHackMe

https://tryhackme.com/room/tutorial

Linux Fundamentals

https://tryhackme.com/module/linux-fundamentals

Other Learning Environments

https://portswigger.net/web-security

https://www.hackthebox.eu/

https://overthewire.org/wargames/

https://underthewire.tech/

Training Rooms

In case it is not clear on TryHackMe, the suggested completion order for the set of the training rooms is:

1. Network Discovery

2. Web Hacking with Burp Suite – Burp on päivittynyt ja sisältää selaimen. Sertifikaatin rekisteröintiä ja proxyasetuksia ei siis enää nykyään tarvitse tehdä, eli voit kuitata taskit 1-3 tehdyksi ja jatkaa kohdasta 4. Jos sisäisen selaimen käyttö antaa sandbox-virheen, laita ruksi välilehdelle Settings → Burp's Browser → Allow Burp's browser to run without sandbox.
3. Web Hacking with OWASP ZAP
4. Upload Vulnerabilities
5. Exploiting with Metasploit
6. Linux Privilege Escalation
7. Windows Privilege Escalation
8. SQL Injections
9. Brute Force login with Hydra
10. Exercise: Vulnversity
11. Exercise: Blue
12. Exercise: Kenobi

Some extra material is available on the topics 1 and 2, if you feel you'd like to learn more:

1. https://tryhackme.com/module/nmap
2. https://tryhackme.com/module/learn-burp-suite

Additional Topics

Research and OSINT:

https://tryhackme.com/room/introtoresearch

https://tryhackme.com/room/ohsint

Password Cracking:

https://tryhackme.com/room/crackthehash

Reverse Shells:

https://tryhackme.com/room/introtoshells

Cryptography:

https://tryhackme.com/module/cryptography

Everything except the kitchen sink in a compact package:

https://tryhackme.com/room/adventofcyber2

How I approach a simple Linux target

nmap -sV <ip> to get application versions

nmap -sT -p- <ip> to make sure no other ports are in use

Typically a web server is found

gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://<ip>

browse with firefox to found directories and also check robots.txt

If upload form is found, upload a reverse shell

If web applications installed, check exploitdb on web or use searchsploit

Check input fields with sqlmap, obtain cookies with Burp Suite if necessary. Dump database if SQLi found.

Use any found credentials to login using ssh

If none work, do a vulnerability scan:

nmap -sV --script vuln <ip>

and/or

download nmap-vulners from git

nmap -sV --script nmap-vulners <ip>

Go to cvedetails.com and check all CVE:s with CVSS over 5.0.

Get exploit from exploitdb or use metasploit

Once you have shell:

check /home/<user> for user.txt

start a python web server in /opt/PEAS/linPEAS and wget linpeas.sh to the target

run linpeas.sh | tee log (and you can browse the log later with: less -R log)

Check all suspicious SUID binaries and sudoable binaries for exploits available in gtfobins.github.io

obtain root and check /root/root.txt

Write a report

????

Profit

Python2 vs. Python3

When you try to run an attack script written in python and it fails with something like:

print "…..

^

SyntaxError: invalid syntax

It means that the script was written in python 2 instead of python 3. You can try to run using:

python2 scriptname

but it more often than not results in error message:

import requests
ImportError: No module named requests

And trying to install module requests only tells you that it already exists in python 3.

pip install requests

Requirement already satisfied: requests in /usr/lib/python3/dist-packages

No worries! You can still get it working by instead running the command through python2:

python2 -m pip install requests

And then you can continue using the script by running

python2 scriptname

Bits and Pieces

Privilege escalation https://gtfobins.github.io/

Reverse Shells https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md

Exploits https://www.exploit-db.com/

Various tricks https://book.hacktricks.xyz/

Little helpers

Hard to use reverse shell? Try rlwrap, or:

python -c 'import pty; pty.spawn("/bin/bash")'

For more ideas, see: https://zweilosec.github.io/posts/upgrade-linux-shell/

Looking for cross-site scripting issues? Try this payload:

JavaScript://%250Aalert?.(1)//'/*\'/*"/*\"/*` /*\` /*%26apos;)/*<!--></Title/</Style/</Script/</textArea/</iFrame/</noScript>\74k<K/contentEditable/autoFocus/OnFocus=/*${/*/;{/**/(alert)(1)}//><Base/Href=//X55.is\76→

https://brutelogic.com.br/blog/building-xss-polyglots/

Just want to check for extra privileges in Linux without uploading PEAS?

sudo -l

find / -type f -a \(-perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null

getcap -r / 2>/dev/null

Final Report

Target of assessment

Each target machine should contain user.txt and root.txt so you can verify the level of access you have gained. You may note them in your report, but finding them is not part of this assignment.

https://tryhackme.com/jr/target1

https://tryhackme.com/jr/target3

https://tryhackme.com/jr/target4

https://tryhackme.com/jr/target5

https://tryhackme.com/jr/target6

https://tryhackme.com/jr/target7

https://tryhackme.com/jr/target8

Reporting Instructions

Please follow the basic PTES structure as defined in the first lecture. For more information about the reporting standard, please visit: http://www.pentest-standard.org/index.php/Reporting

Please note that we are not utilizing the full reporting structure, and you are not required to give for example risk ratings/profiles nor create roadmaps. Please use the structure below for your report and create a single Word or PDF document containing all the target machines.

- Executive summary
    - Background
    - Achieved goals in general level
    - Recommendations
- Technical part
    - Target Hosts unable to be Exploited
        - Information gathering
        - Individual Host Information
        - Vulnerability scanning
        - Attacks conducted
    - Target Hosts able to be Exploited
        - Information gathering
        - Individual Host Information
        - Vulnerability scanning
        - Attacks conducted

        - Attacks Successful
        - Exploits used
        - Level of access Granted +escalation path
        - Remediation
            - Link to vulnerability section reference
            - Additional Mitigating technique
            - Compensating control suggestion

Please remember that a single target may contain more than one exploitable vulnerability.

Further reading: public pentesting reports

https://github.com/juliocesarfort/public-pentesting-reports/

Murtautumistestauksen lainsäädäntö

Rikoslaki 34 Luku 9 § https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L34

Rikoslaki 38 Luku https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L38

Viestintäviraston määräys 67: 15 § ja 16 § https://www.finlex.fi/data/normit/44046/M67A_2015.pdf

sekä niiden osalta perustelut ja soveltaminen https://www.finlex.fi/data/normit/44046/M67A_MPS_2015.pdf

Kokeen ohjeet

Kokeeseen sisältyy käytännön harjoitus TryHackMessä. Testattavasta koneesta tulee raportoida ItsLearningissä olevaan kokeeseen

- User.txt
- Root.txt
- Exploitation vector
- Escalation path

Kohdekone luodaan dynaamisesti jokaiselle käyttäjälle, ja lipuissa sekä hyökkäysvektoreissa on pieniä eroja.

Kokeessa on myös muutamia kysymyksiä murtautumistestaukseen liittyvästä lainsäädännöstä (kts. erillinen dokumentti).