MACQUARIE
University

Faculty of Science & Engineering

COMP2320/COMP6320 Offensive Security

Workshop Week 7

Learning outcomes for this session

The goals of this week are

- Completing Natas exercises (https://overthewire.org/wargames/natas/) from Level 12 → Level 20
- Continue working with HTB machines

TASK 1. wfuzz.

wfuzz is an enumeration tool for websites. It works in a similar way to gobuster, however it focuses more on what is passed to the web server when requesting a URI. Parameters inside the HTTP header can be "fuzzed", random variations away from a mean to see what effects small changes produce. This is mostly done in conjunction with HTTP `POST` requests.

For more information, see https://tools.kali.org/web-applications/wfuzz

TASK 2. sqlmap.

sqlmap is a tool for performing SQL injections on websites. If a website is vulnerable to SQL injection attacks, sqlmap can identify which database is being used, what the data dictionary of the database is, and perform the injection.

For more information, see https://tools.kali.org/vulnerability-analysis/sqlmap

TASK 3. Overthewire Natas.

Go to https://overthewire.org/wargames/natas/. This website has a number of exercises that will help you learn and explore the basics of web-security. You can work in your team and complete levels 12 to 20.

Your tutor will guide you if you have any question regarding the completion of the levels.

You need to prepare a report once you completed the levels. You can use Microsoft Word or any other tool, or indeed you can install a free office suite such as Libre Office within your Kali VM.

TASK 4. HTB FluxCapacitor Machine.

In this task, you will work on FluxCapacitor machine, that is, available at https://www.hackthebox.eu/home/labs/dedicated/315. FluxCapacitor focuses on intermediate/advanced enumeration of web applications as well as bypassing web application firewall rules. Overall, FluxCapacitor is not overly challenging and provides a good learning experience for fuzzing HTTP parameters.
To successfully capture the flags, the following skills are required:

- Intermediate knowledge of Linux
- Knowledge of basic web fuzzing techniques
- Enumerating HTTP parameters
- Bypassing basic WAF rules
- Exploiting NOPASSWD

Note. Your tutor will guide you if you have questions regarding FluxCapacitor machine.
In case you need additional hints, you can refer to FluxCapacitor's write-ups at https://www.hackthebox.eu/home/machines/writeup/119.

TASK 5. HTB Falafel Machine.

In this task, you will work on Falafel machine, that is, available at https://www.hackthebox.eu/home/labs/dedicated/315. Falafel is a challenging machine and requires several unique tricks and techniques in order to successfully exploit it.
To successfully capture the flags, the following skills are required:

- Basic/intermediate knowledge of SQL injection techniques
- Intermediate/advanced knowledge of Linux
- Boolean-based SQL injection
- Exploiting system file name restrictions
- Exploiting video group permissions
- Exploiting disk group permissions

Note. Your tutor will guide you if you have questions regarding Falafel machine.
In case you need additional hints, you can refer to Falafel's write-ups at https://www.hackthebox.eu/home/machines/writeup/124.

TASK 6. HTB Mango Machine.

In this task, you will work on Mango machine, that is, available at https://www.hackthebox.eu/home/labs/dedicated/315. Mango is a medium difficulty Linux machine hosting a website that is found vulnerable to NoSQL injection. The NoSQL database is discovered to be MongoDB, from which we exfiltrate user credentials. We can use one set of credentials to gain a foothold using SSH, and the other to move laterally within the box. A SUID binary is then exploited to escalate our privileges to root.

To successfully capture the flags, the following skills are required:

- Enumeration
- Scripting

Note. Your tutor will guide you if you have questions regarding Mango machine.

In case you need additional hints, you can refer to Mango's write-ups at https://www.hackthebox.eu/home/machines/writeup/214.

Tutorial task.

- Submit the password for Natas Level 19 → Level 20 to iLearn (only the password, no additional text or characters).
- Identify the hash (flag) that is inside the root.txt file in FluxCapacitor, Falafel, and Mango machines, and submit the flags to iLearn (only the flag, no additional text or characters).
- The correct format for your submission is

  `Natas level password, FluxCapacitor root flag, Falafel root flag, Mango root flag`

- Choose one person from your group to record a video of all steps you followed to complete Natas levels in this week. The video recording should have an audio narration. The length of the recorded video should not exceed 30 minutes. Upload the recorded video to iLearn. Each group needs to submit only one video and multiple video submissions will be marked 0.

The deadline for this task is 5pm Friday of Week 8. Your submissions will be assessed by your tutor and it will contribute 2% of your overall grade.

MARKING

Marks will be available in iLearn by the end of Week 9.

Marking guideline is as follows:

Natas level password correctly identified	0.1 Marks
FluxCapacitor root flag correctly identified	0.5 Marks
Falafel root flag correctly identified	0.5 Marks
Mango root flag correctly identified	0.5 Marks
Submitted video	0.4 Marks
Total worth	**2 Marks**

End of Workshop Week 7