University of Portsmouth
BSc (Hons) Computer Science
Second Year

Ethical Hacking (EHACK)

M30239
January 2024 - June 2024
20 Credits

Thomas Boxall
up2108121@myport.ac.uk

Contents

Page 1

Lecture - Introduction to Penetration Testing

📅 2024-01-22 🕘 0900 🎓 Tobi

"If you start searching for Vulnerabilities in WordPress, you will find lots"

1.1 Introduction to Ethical Hacking

Ethical Hacking is the process of finding vulnerabilities and reporting them to the correct people so that they can be rectified. Ethical hacking is a core component of the broader thing which is *Cyber Security*, in which we are striving to protect the three core properties: Confidentiality (protecting information from being disclosed), Integrity (protecting information from being modified) and Availability (ensuring access to information when needed).

1.2 Penetration Testing

Penetration Testing is the continuous process of identifying, analysing, exploiting and making recommendations to vulnerabilities. Pen. Testing is often described as a cycle, which follows a very strict plan within a fixed timeframe.

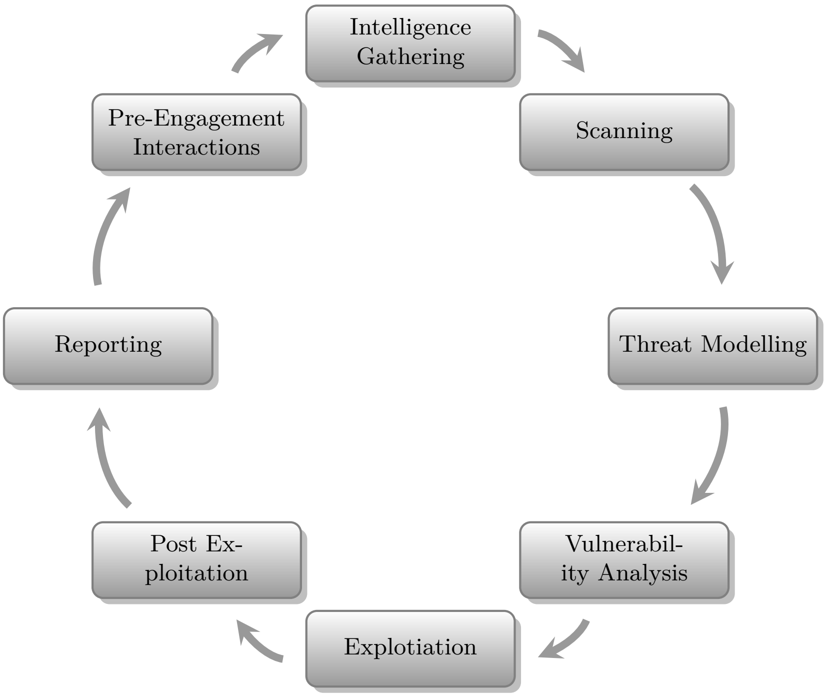

Figure 1.1: Pen. Testing Cycle

There are three types of Pen. Testing:

Black Box where little or no knowledge is disclosed to the pen. tester

Grey Box where some knowledge is disclosed to the pen. tester. They will not be provided full information on anything

White Box where all knowledge is disclosed to the pen. tester

Through Pen. Testing, we actually exploit the vulnerabilities - not just look at them and go “oh, that’s a nice Vulnerability”. Vulnerability assessments can be carried out in a number of places:

Human through human errors, insider threats, social engineering, indifference

Application Functions, storage, memory management, input validation

Host Access Control, memory, malware, backdoor, OS / Kernel

Network Map the network, services, leaks, intercept traffic

1.3 Stages of Penetration Testing

1.3.1 Information Gathering

In the *information gathering* phase, the hacker strives to obtain as much information on the target service / device / company as possible. This could be done through passive methods such as:

- Open Source Intelligence
- Google Dorking
- Social Media Analysis
- DNS Enumeration

Passive methods are methods where as much information as possible is gathered without establishing contact between the pen. tester and the target.

Alternatively, active information gathering techniques (where the pen. tester establishes contact with the target) could be used:

- Open Ports and Service Enumeration
- Directory Scanning
- Common Weaknesses

1.3.2 Exploitation

After gathering information on the target, then next stage is to exploit and vulnerabilities which have been identified. Commonly this can be done through social engineering & fishing, where illiterate users will handover compromising details unknowingly or through known exploits (such as the wp-google-maps exploit explored during the lecture and practical). The decision as to which exploit to use is quite complex and takes a number of factors into consideration including:

- Reliability
- Complexity
- Detection
- Impact
- Environment
- Cost

1.3.3 Post Exploitation

After an exploit has been exploited, the next stage is to see what can be done with the access gained. Commonly this will be to attempt *privilege escalation* through which a basic user account's permissions are escalated to be higher; or to maintain access - which could be done through keeping a SSH session alive or creating a start up service to open a backdoor. The pen. tester will need to cover their tracks, done through editing logs which in linux are found in the `/var/log/` directory. Finally, the pen. tester will write a report detailing what they have found, how they exploited it and give recommendations on what can be done to close the exploit.

1.4 Defences

There are a number of defences which can be used against hacking:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Regular Testing
- Effective Policies
- Regular Effective Training
- Patch Management
- Threat Intelligence

Page 2

Lecture - Information Gathering

📅 2024-01-29 🕘 0900 🎓 Tobi

2.1 Active vs Passive

There are two approaches which can be taken to Information Gathering: Active and Passive. The difference between the two is about the contact the hacker has with the target; where in active information gathering - the hacker has direct contact with the target (which will lead to potential discovery by the target of the hacker) whereas in passive information gathering - the hacker does not make direct contact with the target (which is less likely to lead to discovery).

Active information gathering makes use of probing the network, social engineering, directory & share scanning.

Passive information gathering makes use of: OSINT, search engines, and physical observations. Passive information gathering also includes activities such as DNS enumeration, which can include using whois, IP address scanning and examining associated devices.

Page 3

Lecture - Exploitation

📅 2024-02-05 🕘 0900 🎓 Tobi

3.1 Vulnerability Scanning

The process of vulnerability scanning for a system is essentially scanning the open networking ports & scanning through common directory names to see if anything is found. The outcome from a port scan is a banner grab, which allows hackers to be able to identify the services running and therefore identify any potential vulnerabilities.

The outcome from directory scanning would be revealing a hidden file which hasn't been indexed or finding a misconfiguration. Either of these could lead to identifying further information about the target system that may expose a backdoor.

Listed below are some types of vulnerability scans:

Network-Based Scans identify possible network security attacks and vulnerable systems on networks

Host-Based Scans finds vulnerabilities in workstations, servers, or other network hosts and provides visibility into configuration settings and patch history

Wireless Scans identifies rogue access points and validate that a company's network is securely configured

Application Scans detects known software vulnerabilities and mis-configurations in network or web apps

Database Scans identifies the weak points in a database

Ideally corporate environments will have a patch management system, end user protection, intrusion detection systems and intrusion prevention system. Unfortunately, in reality - this is commonly not the case, especially where there is little-to-no investment in IT infrastructure.

3.2 The Trusted Input Problem

A problem which has plagued digital services for as long as they have existed, is the requirement for users to be able to input data into them. Users cannot be trusted with a text-input field and as such we have to treat everything users input as suspicious until we can prove that it isn't.

Software usually relies on interactions with users and other applications, and data & code are executed in the same location. This can lead to: SQL injection, Stack Buffer Overflow, Shell Code Injection, File Inclusion or XSS attacks.

We can identify vulnerabilities in a number of places: where the data is stored, where the data is processed or where the data is transmitted. The first stage to identifying a vulnerability is to find the injection point - which could be done through an information gathering technique.