Ethical Hacking

The aim of this session is to provide an appreciation of the early stages of penetration testing – namely footprinting and reconnaissance, scanning, enumeration and vulnerability assessment.

WARNING!
Be VERY careful about using these tools – they are very powerful tools that can damage the local network, the University network and the Internet. Please only use the tools described in this tutorial. Misuse of these tools is against the law.

Footprinting & Reconnaissance

The objective of this stage is to identify and extract information about the target organisation. This includes obtaining information about:

- Organisation – e.g. employees, web links, web technologies, patents
- Network –e .g. domains, sub-domains, network blocks, IP addresses of reachable systems, whois record, DNS records

From a passive Footprinting perspective, the University of Plymouth is being used as an example. When looking to perform any form of active Footprinting (or subsequently scanning and vulnerability assessment, **our own internal infrastructure** will be used to ensure we do not compromise wider University systems.

Task 1: Using a search engine, what can you establish about the University as an organisation?

- Identify key personnel (e.g. Vice-Chancellor, Head of Finance, Head of Human Resources, Head of IT).
- Identify additional information about each individual. To save time, focus the analysis on **Nathan Clarke**
- Identify email addresses, telephone number (work/mobile), office/home address, relationship status, children, pets
- Try publicly available databases – Companies House?

Task 2: What network information is available?

- Perform a "Whois" search on Plymouth.ac.uk (whois.domaintools.com)
- What class of network does the University have? What is the IP address space? (Google University of Plymouth IP range – look at tracemyIP.org and ipinfo.io). Try using a class B search on the first two octets.
- Try also using www.netcraft.com – resources, site report. Enter Plymouth.ac.uk.
- Use a reverse Whois search on Nathan Clarke – does this reveal any additional information? Does Nathan have an IP address registered? (https://www.reversewhois.io)

WARNING!
The rest of the tasks in this lab will require access to software contained on systems within the Cyber Security & Forensics Lab (SMB101).

Please DO NOT attempt these tasks until AFTER the lecturer has provided a demonstration of how to access and use the tools

Task 3: Open Source Intelligence – Maltego

- The setup, configuration and use of this software will be demonstrated in class (and record via Panopto). **It is important to remember to copy the VM to the desktop before running it! Copy the Cyber Forensics VM to the Desktop.**
- On a new graph, drag the domain entity over into the graph space. Change the website to www.plymouth.ac.uk
- Right click on the entity and select *To Server Technologies* and note the website technologies being used. Why is this useful?
- Once complete, to remove the nodes, select them and delete.
- Try also exploring:
    - To DNS name [Using Name Schema dictio…]
    - To DNS Name – MX (mail server)
    - To IP Address
    - To Location
- The tool provides critical access to information regarding IP addresses of critical systems, server-side technologies, email addresses etc – all of which can aid in later stages of the hack.

Scanning & Enumeration

Having obtained information regarding IP addresses and the network of the target organisation, the next step will to perform port scanning and networking scanning on those addresses.

Whilst scanning itself is not an actual intrusion, but an extended form of reconnaissance in which the ethical hacker is able to obtain more information about open ports and services. However, it is an active rather than passive approach and can only be undertaken with the appropriate permission.

As such, we will NOT be scanning the University of Plymouth systems, and will instead focus upon a number of internal hosts within the security lab. Please only enter IP addresses as directed in the instructions.

Task 4: Scanning and enumeration of services using Nmap – Zenmap GUI

- Using the Cyber Forensics VM, load Zenmap. Zenmap is a front-end to a widely popular open source tool called NMap.

- Also start the Windows XP, Windows 10 and Metasploitable VMs. If the system is slow, run each one separately.
- The Cyber Forensics VM will act as the ethical hacking host machine, with the remaining VMs acting as Targets.
- Note the IP addresses for each machine (e.g. terminal window - ipconfig on Windows, ifconfig on Linux)
- Run at Intense Scan against the three machines individually. Note the results – open ports and services
- Google NMap and run through the manual describing the options available
- As an example of the impact a Firewall has – on the Windows XP machine, disable the firewall and run the intense scan again. Note the difference information provided to the hacker.

Vulnerability Assessment

Having identified the IP addresses, open ports and services that are listening, the ethical hacker now needs to map this against possible vulnerabilities that may be present so that they can be disabled/mitigated as appropriate.

Task 5: Performing a vulnerability assessment using Nessus

- The setup, configuration and use of this software will be demonstrated in class (and record via Panopto)
- Check to see if the VM already has Nessus Essentials installed, if not:
    - Google Tenable Nessus Essentials – Register to obtain activation key (please do this from your own machine and not the Lab machine).
    - Within the Lab Cyber Security VM, download the client and install on the machine
    - When asked to create a username and password, please use student for both
    - Downloading the plugins will take a little time on first use – be patient!
- If installed, run the software and login using student as the username and password
- Select *New* Scan, enter the IP address of one of the Metasploitable system and click Launch.
- Click scan and Go. The assessment will take a little time – be patient.
- Review the results and explore the vulnerabilities

Task 6: Vulnerability assessment research

- Vulnerability research is critical to follow up on the reports provided by the automated tools. Take a look at the follow sites and explore recent and well-known vulnerabilities.
- Common Weakness Enumeration – identifies types of software weakness (cwe.mitre.org)
- Common Vulnerabilities and Exposures – unique identification of each known vulnerability – common language and approach (cve.mitre.org)
- National Vulnerability Database (NVD) (nvd.nist.gov) – draws CWE, CVE and CVSS (Common Vulnerability Scoring System) to provide a detailed over and status of each CVE.

Exploitation, pivoting and maintaining access

The final stages of an ethical hack. The extent to which these steps are undertaken very much depend upon what the client organisation wishes to achieve. Exploitation often has a direct impact on the systems that are being probed (resulting in operational systems hanging, restarting and the ethical hacking team having access to and control of systems).

Once an exploit has been executed, it is important that the hacker is able to maintain access to continue to achieve their objectives (e.g. exfiltration of data). This will lead to the installation of rootkits, backdoors and pivoting to other systems.

Unfortunately, this is outside of the scope of the lab today. It is important when using this software, the ethical hacker has a full appreciation of what is happening and how systems can be impacted – which is beyond what can be covered in this single session. It is the focus of a whole module in the final year of the BSc (Hons) Cyber Security programme.