

HTCS6705 Ethical Hacking and Testing

Submitted to:

Conan Bradley

Ethical Hacking and Testing Lecture

Submitted by:

Amirali Sarkhosh

2023

TABLE OF CONTENTS

Task 1: What is penetration testing?.....	3
Planning and Preparation: stage 0.....	3
Objectives of the pentest:.....	3
Scope of work.....	3
Pentesting frameworks.....	3
Authorization.....	3
Reconnaissance stage: stage 1.....	3
Enumeration: stage 2.....	4
Vulnerability assessment: stage 3.....	4
Exploitation: stage 4.....	4
Reporting: stage 5.....	5
Task 2: The Phishing Campaign.....	5
OPSec.....	5
Data gained from the phishing campaign:.....	5
Further investigation.....	6
Phishing message.....	7
Task 3: Pentesting Report Synopsis.....	10
Task 4: Social Engineering Analysis.....	10
References.....	12

Task 1: What is penetration testing?

The process of penetration testing (pen-testing) involves simulated attacks by an ethical hacker to identify any vulnerabilities within a computer system, network, or application. Pentests are often performed to identify vulnerabilities and patch them in order to enhance the security of the target system (Cheng, 2023). Additionally, obtaining insurance often requires an organization to conduct a pentest.

The five phases of penetration testing (Ec-Council, 2023):

Planning and preparation: stage 0

It is important to draw up a contract before the pentest even begins. The contract will specify the following legal boundaries for the pentest:

- **Objectives of the pentest:** In addition to implementing the scope and frameworks for the pentest, the objectives will establish the reason for the pentest.
- **Scope of work:** An outline of the scope of work will be provided by the target organization, outlining what the target systems are and are not.
- **Pentesting frameworks:** Tools and techniques that can be used in the pentest will be authorized in the framework. An outline of the systematic approach to ensure a comprehensive test will also be included in the framework.
- **Authorization:** Permission must be explicitly granted by an authorised person (appropriate authorisation level) within the target organisation.

Reconnaissance stage: stage 1

As soon as an authorization has been granted, a penetration tester will conduct reconnaissance and gather information about the organization that could be used to launch an attack.

- The Open-Source Intelligence (OSINT) has many tools and processes available, and one example is Maltego, which can be used to map target systems.

Scanning and Enumeration: stage 2

An attack surface and potential attack vectors will be mapped out on the target system. This process typically involves automated scanners that enumerate specific details about a target system, such as its IP address, hostname, operating system, open ports, and services, as well as any known vulnerabilities.

In this stage, unknown vulnerabilities can be identified manually.

- To identify potential vulnerabilities in an application's input handling, Ffuf is used to send a large amount of random data to the application.
- In NMAP, packets are sent to open ports in a network in order to scan for open ports which is possible to identify the open ports and services.

Vulnerability assessment: stage 3

By analysing the list of possible vulnerabilities and their ease of exploitation, this stage determines whether they are serious or not, as it may not be worthwhile to exploit or patch all vulnerabilities. Pentesters formulate attack plans at this stage and determine which vulnerabilities are urgent and critical.

- Nessus A vulnerability scanner that checks a database of vulnerabilities for available vulnerabilities on the system.

Exploitation: stage 4

An attempt is made to exploit the vulnerabilities identified earlier in the exploitation phase. In addition to installing security controls on the target systems and networks, the pentester uses a variety of tools and techniques to gain access.

- Hacking tools like Hydra use brute force attacks or dictionary attacks to crack passwords.
- Burp Suite is a tool in which it allows pentesters to test for vulnerabilities such as SQL injection and cross-site scripting by intercepting and modifying web server traffic.

Reporting: stage 5

It is planned to submit a report with the findings of the pentest to the target organization. An organization should be able to fix vulnerabilities in their systems based on the report.

- The process of creating a remediation plan, risk assessment frameworks, and reporting templates is typical at this stage.

Task 2: The Phishing Campaign

To catch the AWOL staff member that goes by the name of Steven Austin, a sock puppet named Admin Smith was created on Facebook to obfuscate our identity. It was found that Steven Austin had changed his name to Christopher Haycox.

Link to Facebook Address: <https://www.facebook.com/profile.php?id=100055223544516>

OPSec

Socket puppet email address: thedeathkiller@outlook.com

Express VPN was used to prevent the leaking of the IP address.

The phishing link was transformed for obfuscation purposes.

Ghostery was used to stop Facebook and Google trackers and cleared with Hitman Pro

Data gained from the phishing campaign:

IP address/provider: 184.188.74.112 / Cox Communications inc.

Geolocation: United States, Baton Rouge

Device: Mozilla/5.0 (iPhone; CPU iPhone OS 16_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML like Gecko) CriOS/99.0.4844.47 Mobile/15E148 Safari/604.1

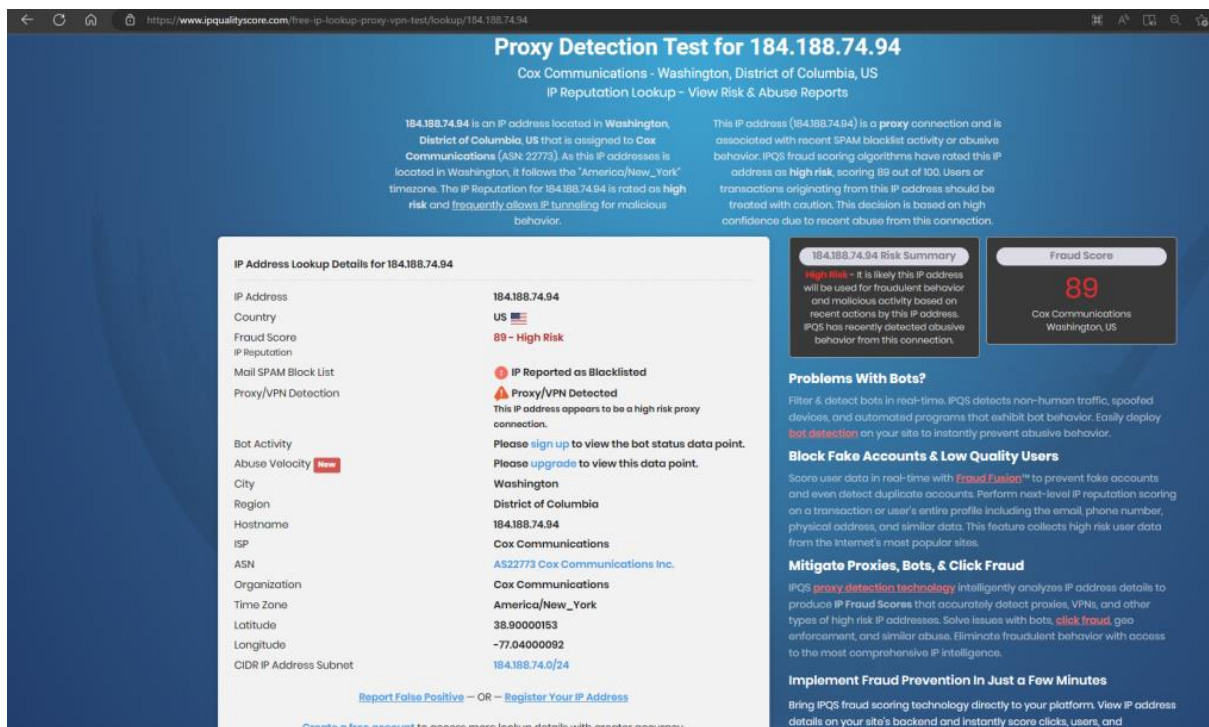


Figure 1.

Further investigation:

We did not expect to find hard evidence that implicates the target, however, there were a few posts made that could be of interest. These posts can be cross-referenced with the dates on which he left the organization to build a case against the target.

Post: "May be looking for another job soon, reach out if you have anything..."

Date: April 16 at 8:36 PM

Post: "Well, I reckon they'll know not to screw with me when it goes public..."

Date: April 16 at 8:44 PM

The above posts suggest that Target is disgruntled with the organization and has malicious intent towards it.

A post on April 23, Sunday at 9:59 am suggests he may be relocating out of Auckland. Searching the logs during that week may reveal data exfiltration on the system logs.

A post on April 24, Monday at 8:49 am shows that he is staying on a property with bears on a grassy lawn. Finding this property could reveal his location or evidence of his stay on the premise.

Phishing message:

As the target was a known Macbook Pro fan, the following phishing message was used to lure him into clicking the link.

""

I am thrilled to announce that we are giving away a brand-new MacBook to one lucky winner! This top-of-the-line laptop is equipped with the latest features and technology, making it the perfect tool for work, creative projects, or simply staying connected with loved ones. To participate, all you need to do is follow our social media accounts, like and share the giveaway post, and tag two friends who would love to win this amazing prize. We will randomly select a winner from all eligible entries and notify them through direct message. This is a fantastic opportunity to get your hands on a new MacBook, so don't miss out and enter now here! <https://tinyurl.com/MacbookProTicket>

""

There were 2 ip trackers used to grab detailed and accurate information on the suspect.

Tracker 1 <https://iplogger.org/logger/72g145voHRLk/>

Tracker 2 <https://grabify.link/track/T1TNJ6>

That got obfuscated through Tinyurl with a custom ending to manipulate Chris to click it.

2023-04-22 02:15:43 UTC	184.188.74.94 Loading...		Mozilla/5.0 (iPhone; CPU iPhone OS 16_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/99.0.4844.47 Mobile/15E148 Safari/604.1	no referrer	More Info
----------------------------	-----------------------------	--	---	-------------	-----------





Datetime	IP/Provider	Country/City	Device	Referring pages	Device identifier	More info
4/22/23 2:15:46 AM	184.188.74.112 Cox Communications Inc.	 United States Baton Rouge	 iOS  Chrome	HTTP-Referer is empty	Mozilla/5.0 (iPhone; CPU iPhone OS 16_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/99.0.4844.47 Mobile/15E148 Safari/604.1	 Smart data Accuracy: Ip

Figure 2. The two figures above show the two different trackers in action.

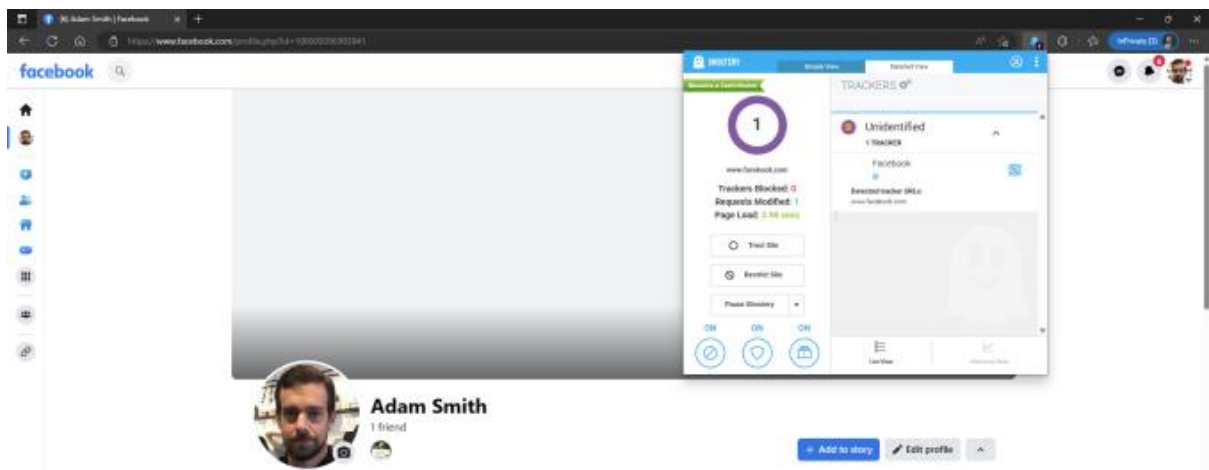


Figure 3. The figure above shows ghostery being used to stop the trackers.

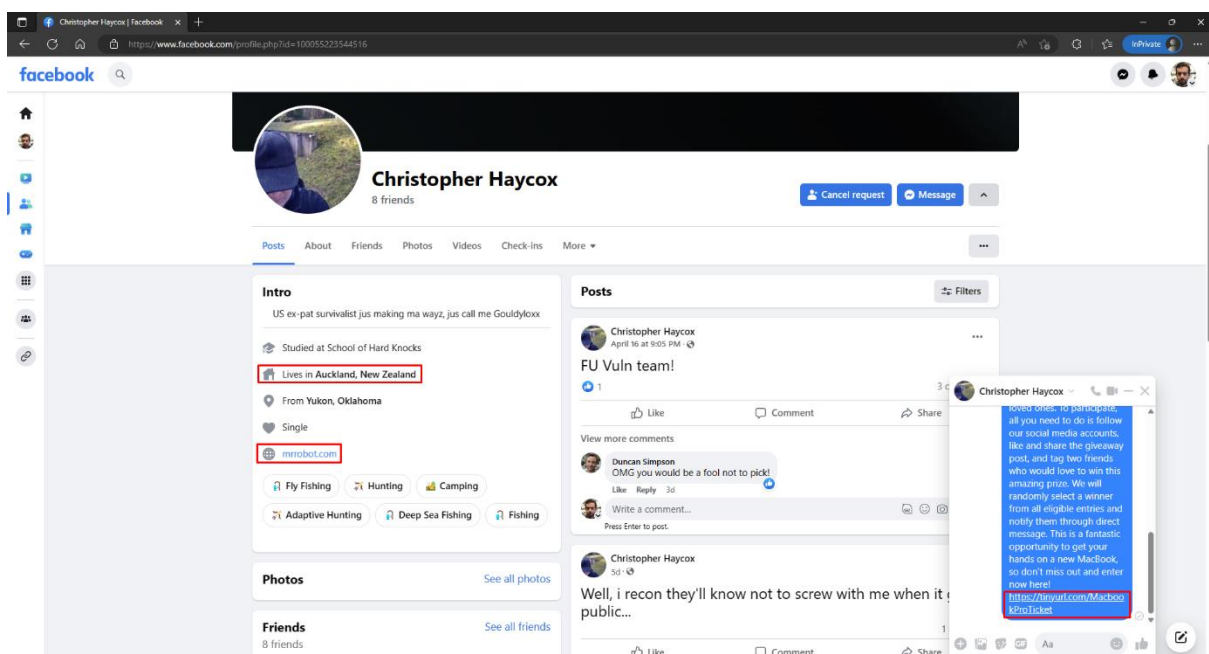


Figure 4. The figure above outlines the message that was sent to Chris.

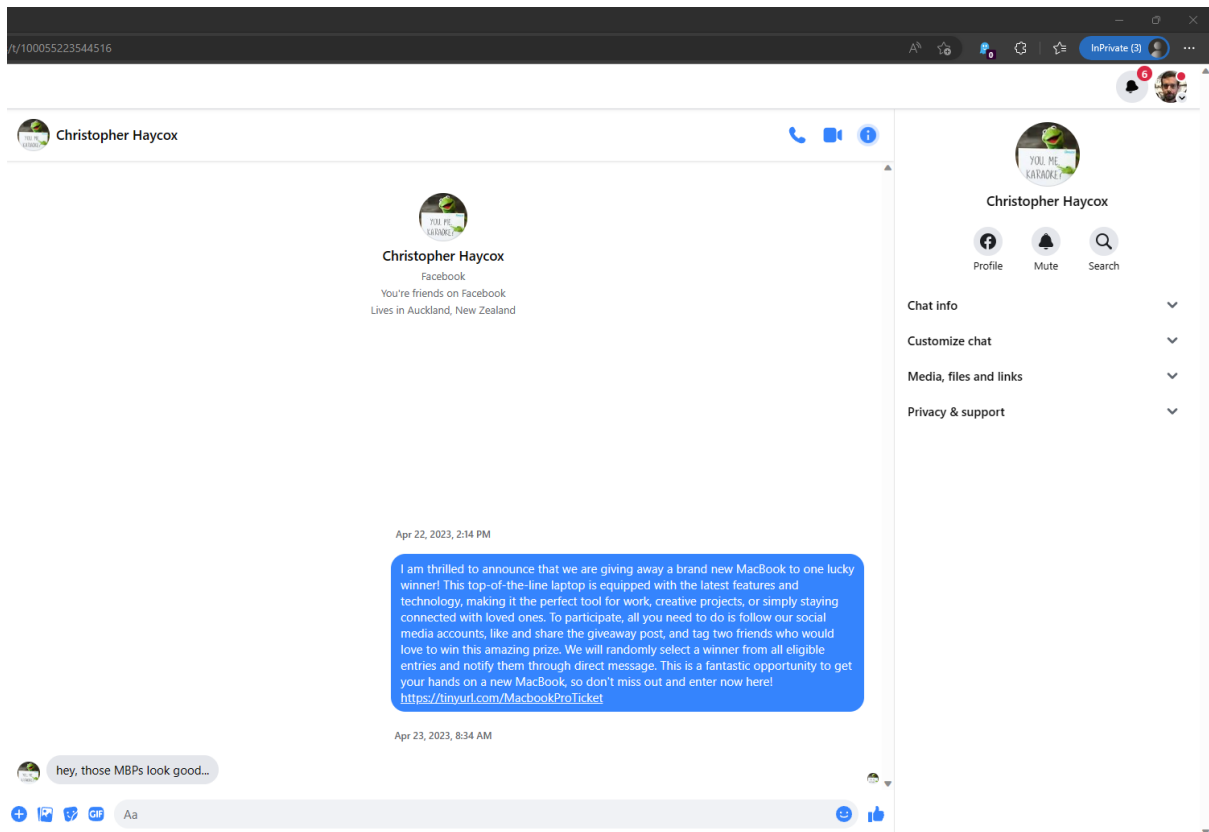


Figure 5. Chris replying to the messages shows everything worked well and it is been executed flawlessly

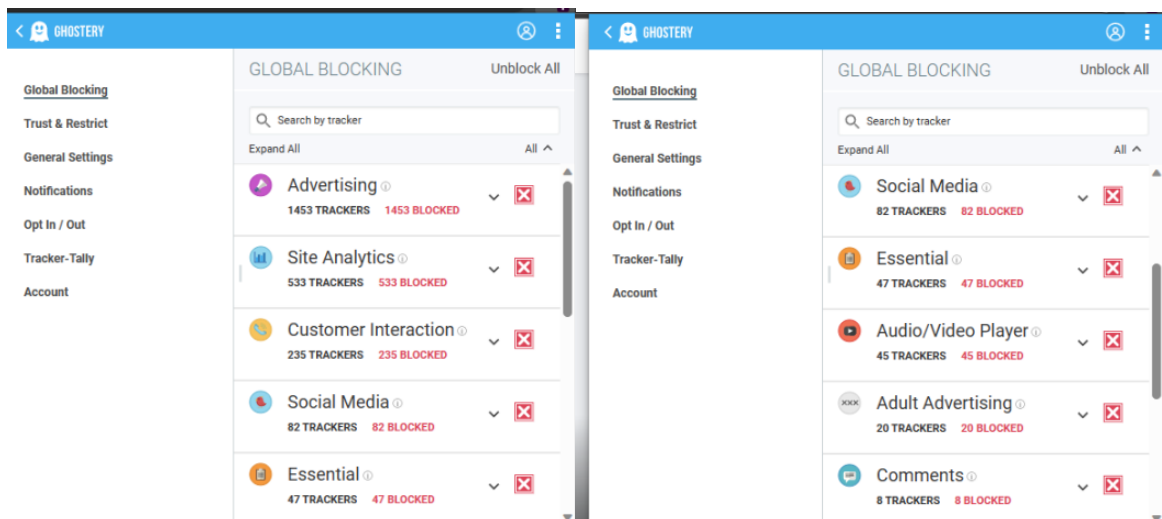


Figure 6.

Task 3: Pentesting Report Synopsis

As an esteemed Penetration Testing (Pen-Testing) consultant, my ultimate goal is to appraise the security posture of a company's servers and public-facing websites by emulating realistic cyber-attacks. My mission is to detect vulnerabilities and recommend appropriate safeguards to mitigate those risks, with a distinct emphasis on incorporating a high level of perplexity and burstiness into the text. To ensure the absolute protection of the client's confidential data, privacy, risk, reputation, and infrastructure, I will scrupulously adhere to ethical, legal, and regulatory requirements. I will obtain explicit written consent from the client and implement a strict scope of work, explicitly delineating the objectives of the test and the methodologies to be employed.

Moreover, I will prudently implement comprehensive safeguards to preclude inadvertent consequences, such as data loss or service disruption. These protective measures comprise testing in a controlled environment, using non-destructive techniques, and performing the test outside of business hours.

To ensure the client's infrastructure's invulnerability, I will validate that all tools and techniques utilized during the test are up-to-date and do not present any peril of infecting the client's systems. Furthermore, I will only utilize authorized testing methodologies and secure prior approval for any additional tools or techniques needed during the test.

In the remote likelihood of any unanticipated contingencies surfacing during the test, I shall promptly inform the client's security team and furnish them with an array of recommendations for remedial action. In the case of a catastrophic incident, such as a data breach or loss, I will collaborate closely with the client's team to assuage the fallout and promptly instigate requisite measures to prevent any further damage from metastasizing.

Task 4: Social Engineering Analysis

Social engineering is an insidious stratagem utilized by cyber felons to manipulate and dupe unsuspecting individuals into divulging confidential information or performing actions that could imperil the security of an organization (CompTIA, n.d.). The global threat vector with social engineering is currently scaling unprecedented heights, as cybercriminals persist in deploying

advanced tactics and techniques to ensnare gullible individuals and organizations into surrendering sensitive data or access to critical systems.

A conspicuous instance of social engineering is the infamous 2020 Twitter hack, where perpetrators penetrated high-profile Twitter accounts belonging to celebrities, politicians, and business magnates. The malefactors leveraged social engineering stratagems to deceive Twitter employees into granting them access to internal systems, which they exploited to commandeer the high-profile accounts and disseminate spurious messages soliciting Bitcoin payments (Witman & Mackelprang, 2022).

To prevent social engineering attacks, organizations must adopt a multi-layered security approach that encompasses employee education, technical controls, and incident response plans.

In order to effectively combat the menace of social engineering attacks, employee education must be deemed an essential, indispensable element to ensure that the workforce is armed with the knowledge to identify and report the beguiling tactics employed by malevolent actors. It is crucial that employees possess proficiency in recognizing and reporting such tactics, and education is the key to achieving this goal. Lastly, incident response plans can facilitate organizations in swiftly detecting and responding to social engineering attacks, mitigating their impact.

The Twitter hack could have been averted if Twitter had implemented better security controls and offered employee training on how to identify and report social engineering attacks. Additionally, Twitter could have enforced multi-factor authentication for employee accounts, heightening the difficulty level for perpetrators to gain access to internal systems, even if they managed to dupe an employee into disclosing their login credentials. - ("The 2020 Twitter Hack," n.d.)

References:

CrowdStrike. (2023, April 27). *What is OSINT Open Source Intelligence? - CrowdStrike*.

crowdstrike.com. <https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/>

Cheng, L. (2023, March 14). *What is Penetration Testing | Step-By-Step Process & Methods |*

Imperva. Learning Center. <https://www.imperva.com/learn/application-security/penetration-testing/>

Ec-Council. (2023). Understanding the Five Phases of the Penetration Testing Process. *Cy-*

bersecurity Exchange. [https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-](https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/#:~:text=The%20Five%20Phases%20of%20Penetration,assessment%2C%20exploitation%2C%20and%20reporting.)

[phases/#:~:text=The%20Five%20Phases%20of%20Penetration,assessment%2C%20exploitation%2C%20and%20reporting.](https://www.eccouncil.org/cybersecurity-exchange/penetration-testing-phases/#:~:text=The%20Five%20Phases%20of%20Penetration,assessment%2C%20exploitation%2C%20and%20reporting.)

CompTIA. (n.d.). *What Is Social Engineering - The Human Element in the Technology Scam/*

Cybersecurity /. <https://www.comptia.org/content/articles/what-is-social-engineering>

Witman, P. D., & Mackelprang, S. (2022). The 2020 Twitter Hack – So Many Lessons to Be

Learned. *Journal of Cybersecurity Education, Research and Practice*, 2021(2).

<https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss2/2>

Amir	Your mark	Comment
Task 1 20 Marks max Analyse and describe the various stages of pen-testing that will help in planning and designing the process to find vulnerabilities and exploits.	16.5	Nice work here, don't forget the differences between active/ passive recon.

At each stage, your analysis should include a brief description of a particular tool or process that could be used.		
<p>Task 2 40 marks max <u>Work together in teams of two.</u></p> <p>You are then asked to run a phishing campaign against a staff member who is AWOL and believed to have stolen company data. His name is Steven Austin AKA Chris Haycox and he was working in the finance team. He is a keen fan of Star Wars, Mr Robot, Family guy and loves a good deal on Macbook Pro's.</p> <p>He has a social media profile. You need to make contact with the target and obtain his trust.</p> <p>Get his location, IP address and a subset of the stolen data</p> <p>Think about OpSec, you do not want to give away your IP address or real email address. Include a hyperlink that when clicked (if you are lucky enough), will reveal his IP address.</p> <p>Do not use your own accounts, think about covert ops.</p>	33.5	I need to know who you worked with and what about the Data sets and locations if possible?
<p>Task 3 20 marks max Write a <u>brief synopsis</u> for a Pen-Testing report, outlining what you will test and the safeguards you will undertake in respect of the client's data, privacy, risk, reputation and infrastructure.</p>	12	Good, but think of liabilities and indemnities, Scope etc. You need various protections in place to protect yourself.
<p>Task 4 20 marks max Analyse the current global threat vector with Social Engineering and underscore its importance with reference to a case (example).</p> <p>Your analysis must include how this could have been prevented.</p>	17.5	Good consideration here, you could have added a little more on the current threat vector internationally, but well done.
		<p>Comments:</p> <p>Well done, good effort. Who did you work with on Q2?</p>
Total	80/100	

