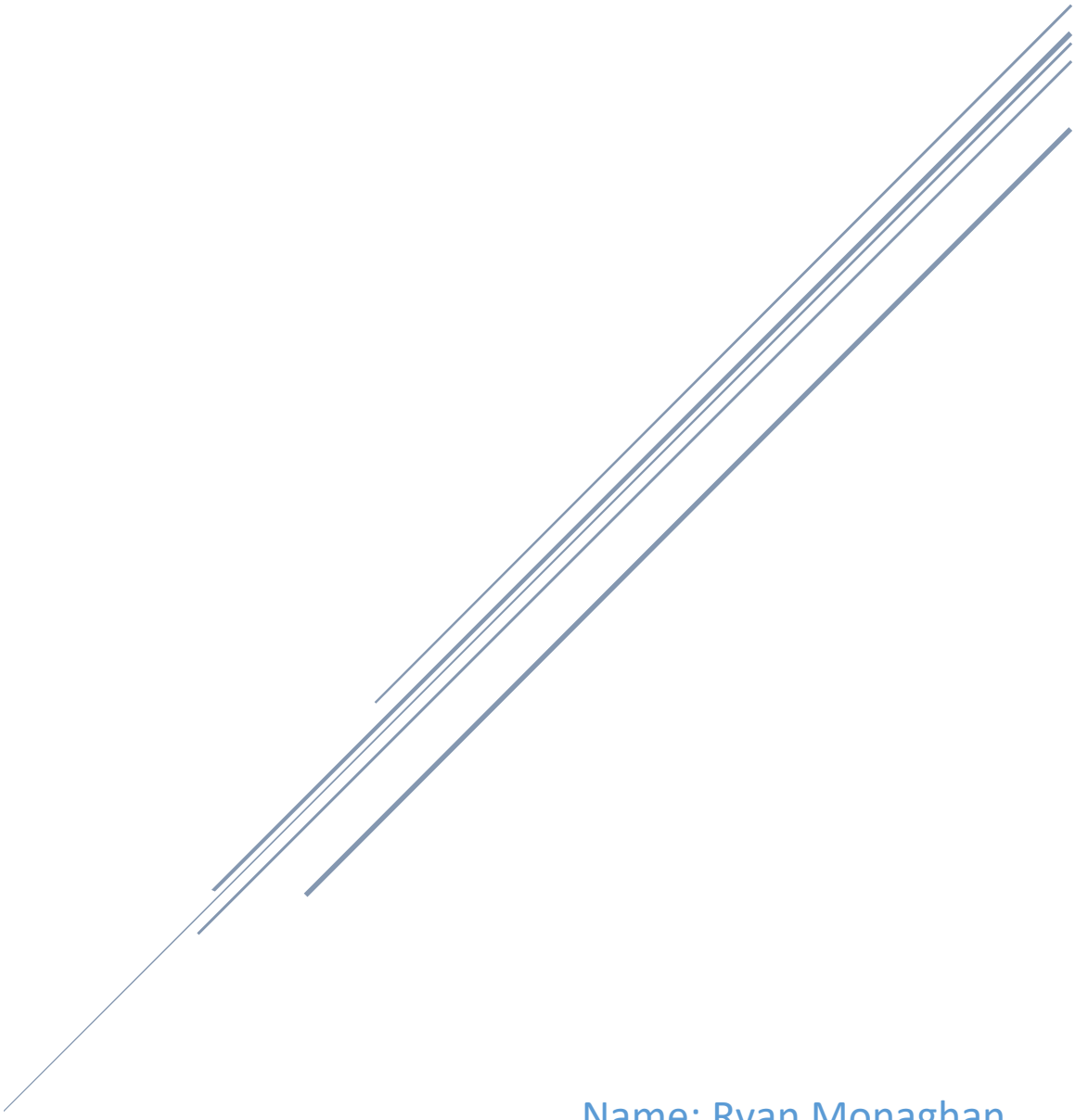
SECURITY PENETRATION TESTING



Name: Ryan Monaghan
ID: R00115129

Contents

Introduction

Overview

For penetration tests that are conducted within the network boundaries passive and semi-passive reconnaissance do not fall within the scope of the test. These activities can, however, often reveal significant information disclosure by the target organization which may inform latter activities. This section of the assignment will assess your skills and knowledge of the reconnaissance and scanning stages of a network pen test.

The aim of this assignment is to take on the role of a member of a penetration tester. The company I have chosen is "Independent News & Media. (INM)".

TASK(S)

For a well-known organization use passive and semi-passive reconnaissance tools and techniques to:

1. Find the human HVTs in the organization (board of directors, CEO, CTO, CFO etc.)

2. Find IP ranges and externally facing servers, webserver version and OS

3. Find staff email addresses, web sites associated with the organization, phone numbers associated with the organization, social groups that are associated with the organization, companies and organizations associated with the organization Use any/all tools detailed in the lectures and any others available that you may find to improve your information.

Who are Independent News & Media?

In order to create a security report, it is important to understand the type of business a company conducts, as it will help link which vulnerabilities will target them specifically.

Independent News & Media are a media group based in Dublin, and are widely regarded as the largest newspaper group in Ireland. INM are responsible for publishing ***"five market leading national newspapers"*** and ***"14 regional newspapers"***. (Source - Independent.ie)

INM also have stakes in job board, property, and matchmaking industries through FindaJob.ie, Globrix.ie and TheMeetingPoint.ie respectively.

Whilst most of INM's published newspapers are sold in stores across Ireland, they also have an online presence for their national papers, where users can keep up to date with news online.

Although based in Ireland's capital of Dublin, INM also have an international presence, again mainly in the media industry. INM subsidiary companies can be found in over ***"22 individual countries, spanning four continents."*** (Source - Independent.ie) Since INM is such a large corporation, and have such a large presence across the globe, I will be refining my security report to four markets, the Republic of Ireland, the United Kingdom, Australia and New Zealand.

INM Company Overview

As Independent News & Media act as a parent company, and house quite a number of subsidiaries, I have decided to refine the company into smaller sections. I have chosen the most popular newspapers of four countries around the world which you can find listed below.

Republic of Ireland

INM - INM.ie & INMPLC.com

Irish Independent - Independent.ie

Sunday World - SundayWorld.com

The Herald - Herald.ie

The Star - TheStar.ie

United Kingdom

British Telegraph – Telegraph.co.uk

Independent UK - Independent.co.uk

Australia & New Zealand

APN - apn.com.au

New Zealand Herald - NZHerald.co.nz

Identifying High Value Targets within INM

Name	Role	Overview	Tenure
Michael Doorly	Chief Executive Officer	Mr. Doorly has been with INM for over 20 years, where he has held a number of senior executive roles, most recently that of Company Secretary and Chief Risk Officer. Before joining INM, he worked in Technicon Ireland Limited (now Bayer Diagnostics) and KPMG. A graduate of UCD, Mr. Doorly is a qualified Chartered Accountant and Chartered Director.	October 2017
John Bateson	Non-Executive Director	Mr. Bateson is Managing Director of International Investment and Underwriting (IIU) and represents IIU on the boards of various companies, both private and publicly quoted. Since joining IIU in 1995, he has been closely involved in the creation of its current portfolio of investments. Prior to joining IIU, John spent six years with the corporate finance arm of NCB Group. He is a graduate of Trinity College Dublin and, having qualified as a chartered	March 2018

		accountant with KPMG, is a Fellow of the Institute of Chartered Accountants in Ireland.	
Fionnuala Duggan	Non-Executive Director; Chairman, Remuneration Committee; Member, Nomination & Corporate Governance Committee; Member, Audit and Risk Committee	Ms. Duggan is Managing Director of KNect365 Learning, part of the events and conferences division of London-quoted Informa plc. A senior digital executive and leader, Fionnuala has enjoyed success in repositioning traditional industries for the digital age, and in establishing and scaling up digital businesses of many kinds inside global organisations. Prior to Informa, she held senior executive roles at CourseSmart, Random House Group, EMI Music plc and Macmillan Publishers. A graduate of Trinity College Dublin and INSEAD, Fionnuala is currently a Governor and Member of the Finance and Resources Committee of London Metropolitan University and a Trustee of Yale University Press (London).	March 2018
Murdoch MacLennan	Non-Executive Director	Mr. MacLennan is Deputy Chairman of the Telegraph Media Group and was previously its CEO for 13 years. Before joining the Telegraph, he was Group Managing Director of Associated Newspapers and, prior to that, Managing Director of the Daily Record and Sunday Mail. He is currently Chairman of the Press Association Group and Chairman of the Scottish Professional Football League. Between 1997 and 2003 he was President of IFRA, the global association for newspapers, and is now a member of the Board of the International News Media Association (INMA). Since 2016, he has been a member of the Council of Google's Digital News Initiative (DNI).	March 2018
Kate Marsh	Non-Executive Chairman	Ms. Marsh is a senior media executive and has built and managed significant businesses across Europe. Working in a customer-focused, highly-regulated environment, she has led mergers & acquisitions, commercial strategy, significant rights negotiations and digital transformation. Ms. Marsh brings strategic and operational experience in brand building and consumer engagement for global companies, most recently from her role as executive vice president for Western Europe International Networks at Sony Pictures Television, and also in various roles at Sky, GroupM and the BBC, joining the Corporation as a journalist. Ms. Marsh has served at board level for Sony Pictures Entertainment regional companies, Plato Media Ltd (home of the pre-school kids App, Hopster) and has been a committee member of the UK's Commercial Broadcasters Association, representing industry to Government.	January 2019
Triona Mullane	Non-Executive Director; Member,	Ms. Mullane has occupied a number of senior roles across technology companies. She was formerly Chief	2012

	Nomination and Corporate Governance Committee	Technology Officer for NewBay Software from 2007 to 2011 (acquired by Blackberry) and previously Chief Technology Officer for ANAM Mobile Limited (from 2003 to 2006). From 1995 to 2003 she was Director of Engineering and subsequently Vice President of Technology for Logica. Ms. Mullane is currently CEO and Founder of mAdme Technologies Limited.	
Kieran Mulvey	Non-Executive Director	Mr. Mulvey has had a distinguished career in public service having been Director General of the Workplace Relations Commission, and formerly Chief Executive of the Labour Relations Commission, for over 25 years until his retirement in 2016 and has served on the governing boards of a number of public bodies including University College Dublin, the Independent Radio and Television Commission and the National Economic and Social Council. He is currently a Director of Dublin City University DAC, Chairman of Adare Human Resources Ltd, Chairman of Sport Ireland and Trustee/Treasurer of the registered charity, the International Foundation for the Protection of Human Rights Defenders. Mr. Mulvey has extensive experience on projects with the European Union and the International Labour Organisation and since his retirement has been engaged by the Government on a number of strategic issues. He is the recipient of Honorary Doctorates from the National University of Ireland and University College Dublin.	August 2018
Dr. Len O'Hagan	Non-Executive Director and Senior Independent Director; Chairman, Nomination and Corporate Governance Committee; Member, Remuneration Committee; Member, Audit and Risk Committee	Dr O'Hagan has extensive national and international management, governance and directorial experience in both the public and private sectors. Dr O'Hagan is Chairman of Northern Ireland Water, Vice President Global Affairs Royal College of Physicians, Chairman All-island Congenital Heart Disease Network Board and a director of a number of private companies. Dr O'Hagan is a former Chairman of Belfast Harbour Commissioners and has held senior positions in a number of international public companies including Fitzwilton Plc, Jefferson Smurfit Group, Independent News & Media (Northern Ireland) and Safeway Ireland of which he was Chairman. He has also been a Director of Waterford Wedgwood UK plc.	2012
Seamus Taaffe	Non-Executive Director; Chairman, Audit and Risk Committee; Member, Remuneration Committee	Mr. Taaffe is an experienced non-executive director and financial and management consultant. He was a Senior Audit Partner with KPMG until his retirement in 2009, as well as being a member of the Board of KPMG Ireland and Chairman of its Consumer and Industrial Markets Group. Since 2012, Seamus has been a non-executive director of Total Produce plc and a member of its Audit Committee.	March 2018

	He is also a director of a number of private Irish companies and a member of two charitable organisations based in Ballyfermot and Tallaght – Candle Community Trust, where he is Chairman, and The Priory Institute.

TABLE INFORMATION SOURCED FROM: https://www.inmplc.com/about-us/board-of-directors

Section One

Security Awareness

In this day and age, it's very important to keep up-to-date with the current malware threats, which can pose menace to companies around the globe. Below I have compiled a list of websites, which I deem give a good insight into the malware threats currently in the wild.

1. **National Vulnerability Database** – The NVD is a trusted database composed by the US government. Users can search the repository for flaws within systems and software. An advanced search is also available, which allows users to take advantage of identifier tags, keywords, and vendors, refining the search results. The repository can be used to reference the INM's current host server OS for possible vulnerabilities.

2. **CVE Details** – CVE Details is the self-proclaimed "*ultimate security vulnerability data source*". Similar to NVD, CVE also allows the user to take advantage of a search engine, where the user can enter the name of specific software they'd like to query. The website then returns all known vulnerabilities for the specific software, be it a browser, a word processor, or an operating system.

3. **Microsoft Protection Center** – Microsoft's official malware encyclopedia allows users to freely search a database profiling all known malware threats. A simple query returns a brief summary of the respective threat, along with a segment dedicated to the technical side of the threat. The technical tab details the threats behavior, symptoms, as well as prevention methods, which could prove useful to security teams.

4. **Symantec** – The fourth and final website I have found is Symantec's Threat & Risk listings. Symantec supply various tools which could be put to use by security teams at INM. The site features an IP lookup, which allows users to lookup the IP of a spam sender, also displaying the spam content type, as well as the category. Symantec also hosts an A-Z database containing specific security threats, as well as response write-ups on each individual threat. This could prove to be a vital asses to any security team due to the vast amount of information and analytical tools supplied by Symantec completely free of charge.

Specific threats of interest to the company

Web Cache Poisoning

Risk Posed - Critical

Since our company is solely media based, and have a large presence in online news, Web cache poisoning poses one of the largest threats to them as a whole. If one of the company's subsidiaries, for example, the Independent, one of Ireland's largest national newspapers was to become a victim of web cache poisoning there would be drastic consequences. The attacker would be able to manually corrupt the web server's domain name system table, and replace it with one of his own. The attacker could redirect traffic to a website hosting malicious threats to

cause even more damage. Since the Independent has such a large online presence the outcome would be drastic, each user would unknowingly be redirected from what they thought was the independent home page, to a possible malicious website. The threat can be removed by simply keeping the server side OS up-to-date. As it currently stands the Independent.ie runs Coyote 1.1, which is known to contain the exploit.

BadUSB

Risk Posed - Critical

BadUSB may take the form of a road apple, a form of social engineering. Universal Serial Ports are present in almost every modern computer system, meaning the vast majority of systems lay vulnerable to this malicious threat. BadUSB may be brought unknowingly by an employee into a corporation, and plugged in to an internal system. They are created by reprogramming the firmware running on a USB. BadUSB is known to be able to

> *"Emulate a keyboard and issue commands on behalf of the logged-in user, for example to infiltrate files or install malware. Such malware, in turn, can infect the controller chips of other USB devices connected to the computer."*
>
> *"The device can also spoof a network card and change the computer's DNS setting to redirect traffic."*
>
> **(Source - https://srlabs.de/badusb/)**

Perhaps the most alarming statement on BadUSB is that is it currently untreatable, and quite difficult to remove. The fact the threat can emulate a keyboard allows if to configure critical portions of the system including the BIOS.

> *"A BadUSB device may even have replaced the computer's BIOS – again by emulating a keyboard and unlocking a hidden file on the USB thumb drive."*
>
> **(Source - https://srlabs.de/badusb/)**

FireSheep

Risk Posed - Intermediate

FireSheep is a browser add-on for the FireFox browser, and is available across Windows, OSX, and Linux. FireSheep uses an integrated sniffer to trace unencrypted cookies from users on unsecure networks. Although FireSheep's threat can be easily prevented by taking advantage of HTTPS, and protected Wi-Fi, users are still vulnerable. For example, a company may allow BYOD, or bring your own device as part of its company policy. If an employee were to connect to an open Wi-Fi connection, which was unprotected, or not using HTTPS, their cookies could be stolen. Cookies normally contain passwords, some of which may display in clear text, allowing easy credential theft. This threat can be prevented by making it common practice to delete and clear cookie caches. Never connect to, open Wi-Fi connections, or enter credentials on not HTTPS secure websites.

Phishing Scams

Risk Posed - Intermediate

Phishing scams usually take the form of e-mails, but can also be conducted over the phone. Phishing scams are often sent out in the masses by botnet clients, usually containing links to hazardous websites, or direct downloads to malicious viruses, worms, or Trojans. They can also be crafted to suit an individual person. This is dome to coerce a victim into parting with otherwise private information.

Ransomware

Ransomware is an example of a malicious type of software usually propagating as a Trojan. Once executed, the Trojans payload is unleashed, which in turn puts the users system into lock down. Users are unable to bypass the ransomware and access their system until a certain condition, usually a financial demand from the attacker is paid, hence the name, ransomware. Ransomware, is usually impossible to remove or bypass, as only the author of the code will have access to the decryption key, forcing the victim to pay the ransom.

Section Two

What is Footprinting?

Footprinting is a method used by an attacker to create a profile, or blueprint of a company they wish to attack. The aim of Footprinting is to gather as much information on a target, in this case, Independent News & Media as possible before conducting an attack.

There are plenty legal ways of obtaining network information from an organization, a few of which I will be talking about through the course of this section. On the flip-side, there are of course illegal methods of obtaining information such as NMaps, which of course I cannot conduct due to the nature of them being, well, illegal.

The first of the legal methods I have used for this report was Whois.

Whois – For this method, I decided to make use of a few websites, Shodan, IEDR & Who.is. Each of these websites are completely open to the public ad free to use. They each supply the user with domain name look-up and IP tools.

Simply entering a URL, will return the user with a plethora of information related to the URL itself. For example, by entering the inmplc.ie URL into IEDR, I was able to obtain the registration dates, the renewal date, holder-type, wipo-status, ren-status, server landing page addresses, nic-hdl as well as the name of the user that registered the domain, in this case, Eamon O'Kennedy.

You can see your whois result below:

% Rights restricted by copyright; http://iedr.ie/index.php/mnudomregs/mnudnssearch/96
% Do not remove this notice

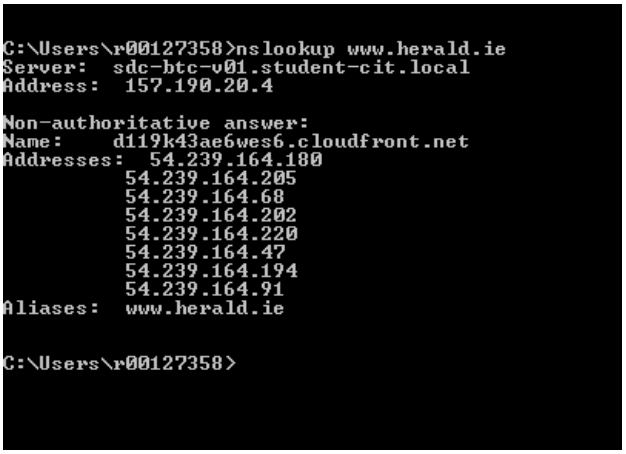
domain: inmplc.ie
descr: Independent News & Media PLC
descr: Body Corporate (Ltd,PLC,Company)
descr: Corporate Name
admin-c: ABB771-IEDR
tech-c: DAD1-IEDR
registration: 08-December-2004
renewal: 08-December-2015
holder-type: Billable
wipo-status: N
ren-status: Active
in-zone: 1
nserver: auth-ns1.iil.ie
nserver: auth-ns2.iil.ie
source: IEDR

person: Eamon O'Kennedy
nic-hdl: ABB771-IEDR
source: IEDR

person: Digihost Ltd
nic-hdl: DAD1-IEDR
source: IEDR

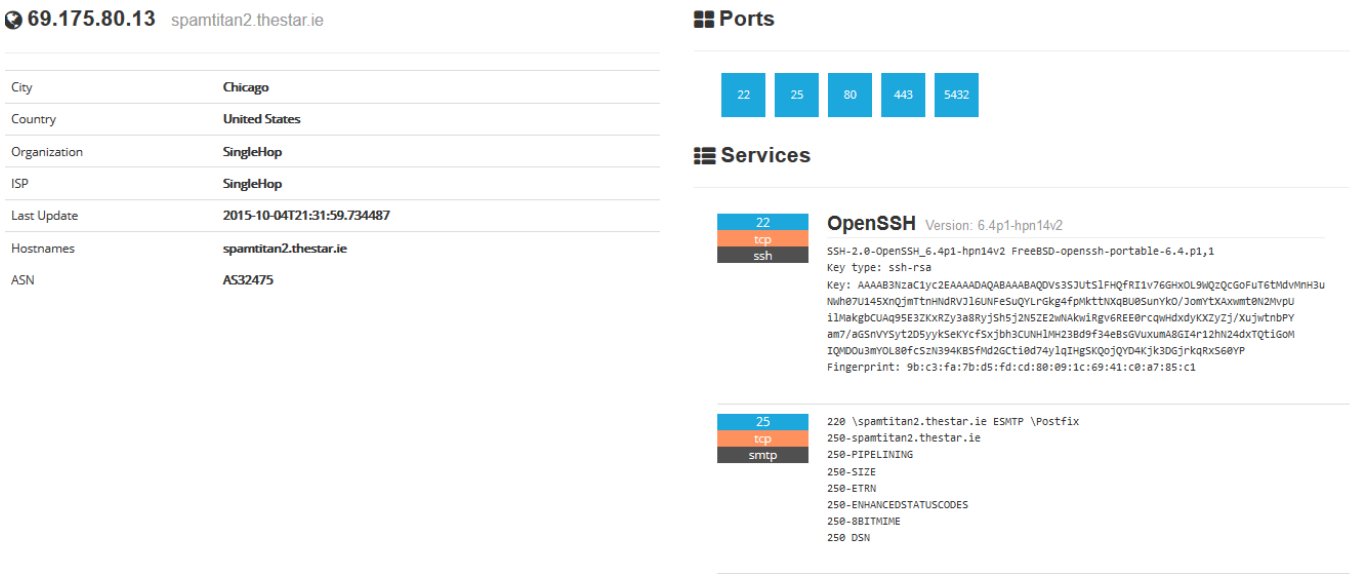
Since INM PLC is a globe spanning organization, they have quite a large footprint when you take into account all the subsidiaries they take ownership of.

I was able to lookup multiple IP addresses by sending NSlookup commands in the command prompt window, built into the Windows Operating system itself. Simply typing NSlookup, followed by a URL returned multiple IP addresses tied to the DNS.



Another method attackers can use as part of the passive reconnaissance phase is port number scanning. In order to obtain the open port numbers for INM subsidiaries, I made use of the tools provided by Shodan.io.

Shodan allows users to enter a URL, or alternatively, an IP address. This allowed me to combine my previously obtained URL's, and combine them with the IP addresses I obtained from the nslookup commands, further increasing network information. For the sake of real estate, I have decided not to include all of the Shodan related screenshots, but an example of one can be found below.



Simply entering the URL inmplc.com, I was able to obtain the location of the server, as well as snippets of information related to it. Open port numbers are also displayed, which attackers can use to their advantage. In this case we can see the following ports are open:

"Port 22 – Secure Shell (SSH), secure logins, file transfers & port forwarding.

Port 25 – Simple Mail Transfer Protocol (SMTP).

Port 80 – Hypertext Transfer Protocol (HTTP).

Port 443 – Hypertext Transfer Protocol over TLS/SSL (HTTPS)

Port 5432 – PostgreSQL database system."

(Source – TCP/UDP Port numbers)

Attackers may use these open port numbers to their advantage. Simply entering a port number, followed by vulnerabilities into a search engine brings back a wide range of results, which attackers may exploit.

Weaknesses & Vulnerabilities

Now that I had found a plethora of information, from open port numbers, to IP's, it was time to find as much weaknesses and vulnerabilities as possible. My first course of action was to try and find the operating systems the host servers were running, and in turn, research vulnerabilities specific to the OS in question.

The first website I visited was Netcraft.com. This site proved very useful, as simply typing a URL into its search feature returned a vast amount of information related to the host server. From an attacker's point of view, this website can be used as a very powerful tool, the website displays information in segments labelled: "Background, Network, Hosting History & Security".

Independent News & Media – Inmplc.com & Inm.ie

Using Netcraft.com, I was able to discover that both inm.ie and inmplc.com were running obsolete versions of Linux Apache 2.4.7 Ubuntu. I ran the version number through CVE's vulnerability database, and 1 public exploit was returned:

"*Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause denial of service, or possibly obtain sensitive credential information or execution of arbitrary code, via a crafted request that triggers improper scoreboard handling*"

Severity – 6.8

(**Source - CVEDetails**)

Given the nature of INM, this sort of vulnerability (Direct Denial of Service) would prove very severe for their subsidiary companies, as a large bulk of their consumers utilize their online news articles. However, given the INM homepage act's as a general overview for the company, a denial of service would not result in a major loss for the company.

Hosting History

Netblock owner	IP address	OS	Web server
A100 US LLC 1919 8th Ave Seattle WA US 98109	54.240.166.4	Linux	Apache/2.4.7 Ubuntu
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	205.251.215.75	Linux	Apache/2.4.7 Ubuntu
A100 US LLC 1919 8th Ave Seattle WA US 98109	54.240.166.4	Linux	Apache/2.4.7 Ubuntu
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	54.192.55.145	Linux	Apache/2.4.7 Ubuntu
US 98108-1226			Ubuntu
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	205.251.206.6	Linux	Apache/2.4.7 Ubuntu
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.0.86	Linux	Apache/2.4.7 Ubuntu
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	54.192.52.203	Linux	Apache/2.4.7 Ubuntu
IIL Web Net	217.78.15.210	unknown	Apache/2.2.16 Debian

Irish Independent – Independent.ie

Again using Netcraft.com, I was able to discover that Independent.ie was running Apache Coyote 1.1, which again, is an outdated version of the OS. The vulnerability in question exposes the web server to web cache poisoning, firewall bypassing and execution of cross-site scripting attacks.

Severity - 4.8

(Source - CVEDetails)

Given the nature of the independent.ie website, most of its audience will be heading to the website to read and browse through news articles. A poisoned web cache can result in the corruption of the servers DNS table. In-turn, this allows the attacker to replace the addressing table, redirecting traffic to domains of their choice.

Netblock owner	IP address	OS	Web server	Last seen Refresh
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.0.243	Linux	Apache-Coyote/1.1	31-Oct-2015
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	54.192.54.230	Linux	Apache-Coyote/1.1	31-Oct-2015
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.0.243	Linux	Apache-Coyote/1.1	31-Oct-2015
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.0.123	Linux	Apache-Coyote/1.1	28-Oct-2015
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.8.11	Linux	Apache-Coyote/1.1	27-Oct-2015
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.8.111	Linux	Apache-Coyote/1.1	26-Oct-2015
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.8.122	Linux	Apache-Coyote/1.1	25-Oct-2015
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.8.126	Linux	Apache-Coyote/1.1	24-Oct-2015
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.8.26	Linux	Apache-Coyote/1.1	23-Oct-2015
Amazon.com, Inc. Amazon Web Services, Inc. P.O. Box 81226 Seattle WA US 98108-1226	54.230.8.35	Linux	Apache-Coyote/1.1	22-Oct-2015

Section Three

Social Engineering

Social Engineering is the term given the manipulation or exploitation of people, in order to gain access to otherwise sensitive or private information. Humans are often looked as the weakest link when it comes to the integrity of a security structure, as neither hardware nor software can protect an individual from being exploited in to leaking sensitive information.

Social Engineering attacks are often conducted on individual employees. Once the attacker has their sights on an employee, the set off to gather as much information they can on an individual. Simply finding a targets social media account usually exposes their personal interests, hobbies, and basic information.

Depending on the victim, phone numbers and email addresses may also be obtained from their social media profile. Once this information has been attained, the attacker could compose an e-mail, and use those hobbies and interests against them, in an attempt to connect with the victim. These specifically arranged e-mails are then used to coerce the victim into leaking private information.

Another method of social engineering that can be used, would be feigning authority or employment. Using this method, and attacker could mask themselves as a member of staff, for example, an IT worker, or an authoritive figure.

The attacker could compose an e-mail, containing a made up situation, such as maintenance on an individual's system, then manipulating them into releasing their login details. Alternatively, this method can also be conducted over a phone conversation, in which the attacker feigns a situation of importance in order to gain access to otherwise sensitive information.

Physical and digital authentication

Physical – INM should update company policy to include compulsory ID, or Magnetic stripe cards. These cards would limit access to certain sections of the building. For example, IT related employees should be the only employees allowed in server rooms, or IT laboratories.

The inclusion of swipe cards limits the population of areas of the building, which in-turn limits the suspect list if a social engineering breach has occurred. Visitors form the public will also have limited roam over the building in this case.

Policy should expel the use of road apple devices. The use of foreign USB, CD-ROM, or Mobile Phones should never be inserted into company systems. Road apples are placed specifically by attackers to catch the attention of an employee, in hopes they will connect the device to a corporate system.

This allows the attacker to bypass the entire security system on the premises, without ever having to enter the building themselves. Road apple devices commonly contain malicious threats which can then cause widespread damage to the company.

Passwords should never be stored, or sent digitally. Passwords should only be delivered in a physical form, which is then memorized and destroyed. They should not be stored in an open area, nor kept on post-it notes on a workstation. Workstation should never be left unattended, even if it's just for a few seconds, systems should be put behind a lock screen.

Digital – Company policy should enforce the use of complex passwords. Users and employees should be forced to change passwords each calendar month.

Employee e-mail accounts should be tied to some sort of two step authentication, such as a token authenticator, or a mobile authenticator, in which the user sent a time sensitive token once the correct credentials have been supplied. Company policy should make unique passwords compulsory, passwords should not be used more than once.

Recommendations on authentication systems to prevent physical access.

As discussed earlier, each area should be sectioned off into different departments. Employees should be given access cards, specific to their employment role. Article composers for example should not have access to the server room. Vital areas to company should be locked behind multi-tiered security authenticators, for example a biometric measure such as a fingerprint, alongside an ownership measure such as an authentication token.

Fingerprints are unique to each individual, replicating them is possible, however, if compromised, an attacker will still have to breach the authentication token.

The authentication token will act as a time slice based key. The authenticator may come in the form of an in-house application designed by the company to display a token on screen. The token appears for a certain period of time, usually 20-30 seconds, before becoming invalid ad displaying a new token. Alternatively, the token distributer could be tied and bound to a phone number. The user is prompted for the last four digits of their company phone number, if correct, the user will receive a time sensitive SMS displaying the authentication token.

Part 2: Active Scanning and Exploitation

Your pentesting company has been hired to perform a test on a client company's internal network. Your team has scanned the network and you have been assigned 4 of the discovered systems. Perform a test on these systems starting from the beginning of your chosen methodology and submit your report to the project manager. These machines can be found in the catalog under “COMP8028 Assignment”.

TASK(S)

The activities of this assignment would occur chronologically after that of Part 1 of the assignment in a penetration test. In this section of the assignment you should approach the systems in this order:

1. Metasploitable 1
2. Metasploitable 2
3. Windows XP
4. Windows 7

Use nmap or equivalent to determine IP addresses of the machines, verify the OS and services on these. You should attempt to find as many entry points into each machine as possible (easy for the first 2). Use a vulnerability scanner (nessus or equiv.) of your choice to scan the vulnerable machines. Identify any false positives in your scan if possible. Use metasploit to exploit your targeted vulnerabilities and explain how you accomplished this.

Bibliography

https://www.cvedetails.com

http://www.netcraft.com/

Computer Security Lecture Notes.

https://www.shodan.io/

http://www.inmplc.com/

https://pwnedlist.com/

https://ie.linkedin.com/

https://www.reddit.com/r/hacking

https://www.reddit.com/r/netsec/comments/2i6vvh/badusb_the_unpatchable_malware_that_infects_usbs/

https://github.com/adamcaudill/Psychson

http://www.techworm.net/2014/11/half-the-usb-devices-world-over-have-badusb-flaw.html

https://srlabs.de/badusb/

http://www.ironkey.com/en-US/solutions/protect-against-badusb.html

CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking by Krutz, Ronald L. & Vines, Russell Dean

https://who.is/

https://www.iedr.ie/

https://nvd.nist.gov/

Microsoft Malware Encyclopedia

https://www.symantec.com/index.jsp