ASSIGNMENT 6

1. Define ethical hacking and distinguish it from malicious hacking, highlighting the importance of ethical consideration

When many people hear the term hacking, it’s often correlated with cyberattacks. However, in today's technology driven world, there’s a group of cybersecurity professionals that essentially hack the hackers – they’re called ethical hackers.

The role of an ethical hacker is important within the cybersecurity industry. Ethical hackers are tasked with the knowledge, skills, and experience to perform risk assessments and test systems for security related issues. These tests are conducted against all possible security breaches, exploits and vulnerability scenarios that protect organizations from attacks.

According to the Bureau of Labour Statistics, the cybersecurity industry will only continue to grow in the coming years. Job projections for roles like **cybersecurity analyst** show a **33% increase in growth** over the next few years. To learn more about types of hackers plus the tools, responsibilities, and certifications needed to become an ethical hacker, continue reading.

Types of Hackers

Using the term hacking or hacker usually has a negative connotation in its definition. Malicious hackers are often highly skilled in coding and programming, and modifying computer software and hardware systems to gain unauthorized access. However, not all hackers are created equal, and they’re not always cybercriminals.

Hacking consists of conducting technical activities with the intent of exploiting vulnerabilities within a computer system, network or firewall to obtain unauthorized access. It involves misusing digital devices such as computers, networks, smartphones and tablets.

The goal of hacking is to manipulate digital devices in order to cause damage or corrupt operating systems. It also allows hackers to collect user information, steal sensitive information and documents or perform other disruptive data related activities.

While hackers can be both ethical and malicious, most fall within three main types of hacking. These three main varieties of hackers are authorized, unauthorized and grey-hat hackers. Each type has different intents and purposes for their exploits. Let's explore each of these types of hackers and how they operate.

Unauthorized Hackers

Unauthorized hackers, also called **black-hat hackers**, are malicious types of hackers. These hackers often use their technical skills and knowledge to seize control of computers and operating systems with the intent of stealing valuable data. Unauthorized hackers will utilize many methods to gain unauthorized access to computer systems and networks to steal sensitive organization or individual data.

Unauthorized hackers are often the criminals behind many significant data breaches and exploits. Most of them commonly use **malware**, **social engineering** and **denial of service** tactics to execute attacks against organizations.

Unauthorized hackers may act on their own, as part of a larger cybercrime organization or on behalf of an enemy nation-state. Most are motivated by reputation, monetary gain, or espionage conducted on both nation-states and corporations.

Authorized Hackers

Authorized hackers, also called **white-hat hackers**, are what many in the information security industry call ethical hackers. While most unauthorized hackers do not follow laws or permissions to target systems, authorized hackers will. They are expected to follow a code of ethics while also following established laws and access permissions when conducting their activities.

Authorized hackers are generally hired directly by companies or clients to test operating systems, hardware and software and network vulnerabilities. They will utilize their hacking knowledge, skills and expertise to help companies improve their security posture from attacks.

Authorized hackers break into systems to **find vulnerabilities** so that companies can patch their systems and mitigate potential cyber threats. They also conduct **penetration tests** as a part of their role. Penetration testing will expose the weaknesses in a network to test its security measures. It can also determine how vulnerable it is to attacks from malicious hackers.

Grey-Hat Hackers

Aside from the **authorized and unauthorized hackers**, there is another type of hacker that is a blend of both. These types of hackers are commonly called grey-hat hackers. Grey-hat hackers are individuals who exploit security vulnerabilities to spread public awareness that the vulnerability exists. While these hackers do not share the malicious intent commonly attributed to unauthorized hackers, they also don’t necessarily adhere to a code of ethics like authorized hackers.

Grey-hat hackers may opt to reveal the security vulnerability privately to the company or manufacturer without publicizing the results. However, many grey-hat hackers will publicly exploit the vulnerability found in hardware or software programs without manufacturer permission to raise awareness of the problem.

A common concern within the cybersecurity industry is that when a grey hat releases an exploit, it makes it easier for malicious hackers to steal information and data from systems.

For instance, a group of grey-hat hackers identified and released a security gap in several models of **Linux routers**. This release resulted in updates for companies and individuals, allowing for closing that security gap. However, the exposure may have also resulted in many attacks on individuals and organizations because the exploit was released publicly.

How Ethical Hackers Differ From Malicious Hackers

Ethical hackers work with companies, the government and other organizations to identify potential vulnerabilities in their systems. This Intel can be used to fix security issues and vulnerabilities before adversaries have a chance to exploit them.

There are several significant other ways that ethical hacking is different from malicious hacking:

- Ethical hackers are hired to test vulnerability and not steal anything from the systems they're testing. Their main goal is to only look for gaps in the system's security defences.
- Ethical hackers utilize several methods to test systems apart from just attempting to gain access through illegal pathways. These paths can include brute force attacks or using key loggers to reveal user-password vulnerability. They will also utilize legal methods of gaining access that mirror real-world attackers, known as the ethical hacking methodology.
- Ethical hackers follow a strict code of ethics when conducting the tests that guide their work. This code prohibits them from sharing how they breached security measures with anyone outside the client or organization. As a result, most companies and organizations are more likely to trust an ethical hacker.

Roles and Responsibilities of Ethical Hackers

Ethical hackers often have job responsibilities that go beyond lawfully hacking systems for security issues. The primary goal of an ethical hacker is to test and identify vulnerabilities in an organization's system and correct them.

Ethical hackers are expected to follow specific guidelines to perform hacking for organizations legally. These guidelines include approval from the system owner before executing the security review.

Some of the additional roles and responsibilities that an ethical hacker will have also include:

- Discovering the operating system and network weaknesses in an organization's technology infrastructure.
- Demonstrating how easy it is to launch cyberattacks on their company using penetration-testing methods.

- Executing security assessment simulations to show how easily they could be hacked by someone else.
- Reporting any security breaches and vulnerabilities discovered within the system or network directly to the owner or manager of that system.
- Keeping the discoveries confidential between them and the client or company.
- Wiping traces of the hack to ensure that malicious hackers cannot enter the system through the identified loopholes.

Skills and Certifications Required for Ethical Hackers

Ethical hacking is a technology career with specific skills, and cybersecurity certifications help people break into the field. Many ethical hacking jobs still require a bachelor's degree in information technology, or another technology or cybersecurity related degree. However more employers are considering candidates without degrees in favor of experience and certifications. The most proficient ethical hackers have a combination of a degree, experience and certifications.

Ethical hackers should also have a working knowledge of infrastructure technology including Linux servers, Cisco network controls, virtualization, Citrix and Microsoft Exchange. Computer programming experience and understanding of various programming languages is required for advanced positions.

Many employers will require ethical hackers to have certifications in addition to their degree and experience. **CompTIA PenTest+** and **Certified Ethical Hacker (CEH)** through **EC-Council** are among the most recognized industry certifications. They cover the skills and knowledge needed by experts in information security and ethical hacking.

Ethical hackers also need strong analytical skills, given that the work involves examining data to identify potential issues. Therefore, to break into this field, you must also have superior problem-solving skills, creative strategy skills and attention to detail. These skills are necessary, as ethical hackers must be thorough in their efforts to breach the security systems.

Regular re-certification is necessary to stay up to date with this industry. Continued education on the latest penetration software and industry recommendations can also be beneficial for ethical hackers in their careers.

Standard Tools Used in Ethical Hacking

A wide variety of tools on the market are used in the field of ethical hacking. Some of these tools include network scanners, penetration testers and more. Below are some of the most commonly used tools ethical hackers utilize in their roles:

Nmap: Is one of the most popular network scanning and mapping tools. Its built-in scripting library can scan for open ports and check for vulnerabilities. It can be used locally and remotely to monitor networks for security gaps. It can also be used on mobile devices and smartphones with root credentials.

Wireshark: Is a protocol analyzer tool that allows you to collect the data from a network without disturbing its ongoing operations. It helps ethical hackers test the network for security flaws. This tool is beneficial to ethical hackers trying to identify what kind of traffic the computer sends/receives while connected online. The only limitation to this tool is that the viewable packets are visible as long as they are not encrypted.

Burp Suite: Is an integrated platform for web security testing that includes proxy server, repeater and intruder mode. It also includes other tools such as Spider, Scanner and Intruder. This tool makes it easy for an ethical hacker to perform various tasks, such as detecting vulnerabilities in websites/web applications. The testing is done while maintaining a high level of security throughout their operation process.

Limitations to Ethical Hacking

Ethical hacking can often have a misunderstood scope and limit within the industry. Although ethical hacking is a type of penetration testing, it uses attack simulations and methods to assess the system and network, reinforcing that there's more to ethical hacking than just penetration testing.

Many ethical hackers need to be multifaced in not only thinking like a hacker but moving like one as well. They need to know how they operate, what they use, and the tools used to employ countermeasures against the system and network vulnerabilities – while remaining within the bounds of the laws and permissions.

Ethical hacking is also often compared with vulnerability or risk assessments. Vulnerability assessment (VA) takes place before penetration testing begins. A VA can scan for security vulnerabilities on a system or network without exploiting them. This is done to determine weaknesses in said system or network before taking further action to mitigate them.

Ethical hacking often involves many different facets of the information security field. This role requires a lot of knowledge and expertise, from coding and programming to penetration testing and risk assessment. There is a lot to learn within the ethical hacking career, but it's a high-demand field that will only continue to grow the more technology is used in our world.

2. Explain the concept of open-source intelligence (OSINT) and its role in information gathering for ethical hacking.

An Introduction to Open Source Intelligence (OSINT)

The internet has changed everything around us from education, healthcare, government interactions reaching social communication which receives the greatest impact. The Internet has redefined how people communicate with each other and revolutionized how corporations do business. Nowadays, the majority of world communications happen in what is known as Cyberspace.

According to *cybersecurity ventures* by 2030, 90 percent of the human population, aged 6 years and older will be online, this means more than

7.5 billion Internet users. People now use the internet to purchase goods & services, entertainment, connect with other people, share information and files in addition to using social networking websites to communicate with friends and family members without any geographical barriers.
As the world continues to digitalize, digital societies will produce huge amount of digital data generated from people and business interactions in Cyberspace. Exploiting this info in the right direction will open numerous opportunities for public and business organizations to increase profits and operate more efficiently in the new information age.

Open Source Intelligence (OSINT) refers to all information that can be found publicly – mostly via the internet – without breaching any copyright or privacy laws. Under this definition, a wide array of sources can be considered a part of OSINT. For instance, information posted publicly on social media websites, posts on discussion forums and group chats, unprotected websites directories and any piece of information that can be found by searching online. Keep in mind that most OSINT resources cannot be found using regular search engines such as Google or Yahoo!, as many resources are buried deep in the deep and darknet and such resources constitute more than 96% of the web content.we will shed the light on the term OSINT, discover its types, actors interested in OSINT gathering and explore OSINT benefits in today's digital age.

What is OSINT?

As we already mentioned, OSINT refers to all the information which is open for public consumption, this includes both online and offline resources. You may wonder, does this information need to be free to be considered a part of OSINT resources? The answer is No, for example, the information contained in scientific papers, books, and magazine need to be purchased first in order to disseminate it in your OSINT gathering activity.

The U.S. Department of Defence (DoD) defines OSINT as follows:

"Open-source intelligence (OSINT) is an intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."
OSINT Types

OSINT can be classified – according to where the public data is found – into the following categories:

1. The internet is the main place where OSINT resources are found, indeed, many researchers differentiate between the online OSINT resources and the offline one by using the term "**Cyber OSINT"** to refer to internet resources exclusively. Internet resources include the following and more: blogs, social media websites, digital files (photo, videos, sound) and their metadata, technical foot printing of websites, webcams, deep web (government records, weather records, vital records, criminal's records, tax and property records), dark net resources, data leak websites, IP addresses, and anything published online publicly.
2. **Traditional media channels** such as TV, radio, newspapers, and magazines.
3. **Academic publications** such as dissertations, research papers, specialized journals, and books.
4. **Corporate papers** such as company profiles, conference proceedings, annual reports, company news, employee profiles, and résumés.
5. **Geospatial information** such as Online maps, commercial satellite images, geo-location information associated with social media posts, transport (Air, Maritime, Vehicles, and Railway) tracking.
   Who needs Open Source Intelligence?

   There are different actors interested in OSINT gathering with varying motivation for each one.

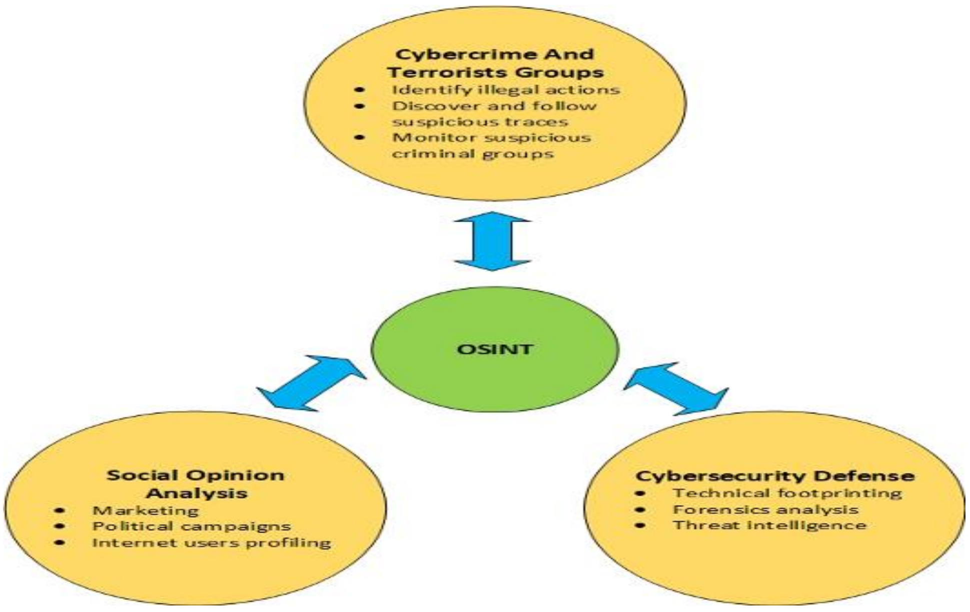


Figure 1 – OSINT is used by different users for different scenarios

Law Firms & Private Investigators

OSINT is used extensively by law firms to optimize their litigation by discovering information found on social media sites and other online places to uncover biases and acquire important information about the individual's or organization in question. The information acquired from public sources can be beneficial in the following cases:

- Discrimination & sexual harassment lawsuits
- Wrongful termination, disability, and hostile work environment claims
- Intellectual property violation cases

Ethical Hacking

IT security professionals utilize OSINT search techniques and tools to discover weaknesses in friendly IT systems, so such vulnerabilities can be closed before threat actors discover them. Commonly found vulnerabilities include:

1. Accidental leaking of sensitive information on social media sites. For example, an unaware employee may post a personal photo in the server room showing the type of security devices used to secure corporate network.
2. Open ports and insecure services running can be discovered when scanning the subject network for vulnerabilities using specialized tools.
3. Outdated operating system versions, software and any content management systems already in use.
4. Leaked information found on data leak repositories or across the darknet.

Gain Intelligence about Competitors Activities

As the internet becomes widely adopted in all life and business areas, corporations can utilize OSINT to gain great insight into current and future threats. For example, OSINT can be used to gain useful intelligence about competitors' marketing and business operations, their deals with other companies in addition to their future plans (e.g. expand to new markets, launch new products or services).

Law Enforcement Agencies

OSINT techniques help Law enforcement officials to improve their intelligence gathering activities to protect citizens and businesses from cybercriminals. OSINT can also utilize in this context to identify possible criminals – by examining their social media accounts and online behavioural – before they commit their crime. For example, law enforcement can use a search algorithm to scan social media sites – and other online public sources sites – for terms like **“shoot”** or **“kill.”** to stop possible criminals before conducting any crime.

Government Agencies

Governments are the greatest consumer of OSINT intelligence; they need such info to predict future trends on a global level. Governments seek professional reports concerning any area of interest (political, health, economic or sports events, etc.) from specialized OSINT firms to help them in their decision-making process.

Individuals

Ordinary people use OSINT to check how much personal information is exposed about them online. This helps them to discover and delete any unwanted information leaked publicly and prevent bad actors from exploiting such info to target them with customized attacks (e.g. Social engineering attacks).

In general, all internet users are using some sorts of OSINT search techniques in one way or another, for example, when using Google to search for something, or when using the search box in Facebook or Twitter to search for someone, you are utilizing OSINT to find this info.

Cybercriminals and Terrorist Organizations

In the bad side, cybercriminals and terrorists are using OSINT techniques in the same way good people use to find information about their targets. Threat actors use OSINT to examine possible targets, identify weaknesses in target computer networks and finally use this intelligence to exploit the target.

OSINT is considered a valuable tool to assist in conducting social engineering attacks. The first phase of any penetration testing methodology begins with reconnaissance (in other words, with OSINT).

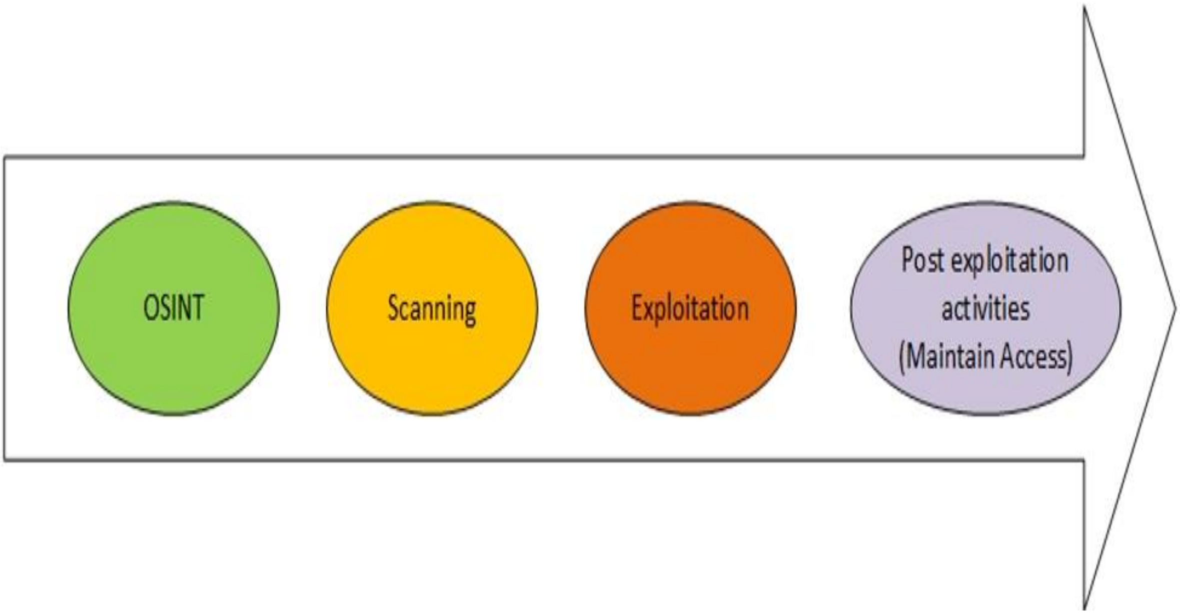
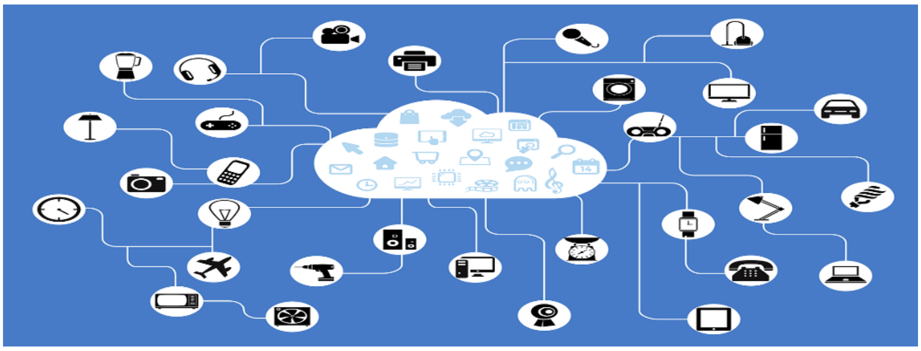


Figure 2 – General penetration testing methodology always begin with OSINT gathering (Reconnaissance)

Pushed by the huge technological advancement and the wide prevalence of internet communication worldwide, OSINT becomes a critical component of both public and private intelligence, supplying businesses, governments, and individuals with a plethora of tools and techniques to gather intelligence from high-quality information to the base and make decisions on. OSINT is beneficial for different scenarios, whether you are conducting an investigation for research, competitor intelligence, vulnerability assessment, threat analysis, or you are simply an individual who cares about his privacy and wants to discover what personal information is already – inadvertently – leaked about him, OSINT will give you the required tools to have access to some of the best available data in the world and mostly for free.

Open Source Intelligence (OSINT): A Practical example



OSINT is the practice of gathering intelligence from publicly available sources to support intelligence needs. In the cybersecurity arena, OSINT is used widely to discover vulnerabilities in IT systems and is commonly named **Technical Foot printing**.

Foot printing is the first task conducted by hackers – both black and white hat hackers – before attacking computer systems. Gathering technical information about the target computer network is the first phase in any penetration testing methodology.

In this I will demonstrate how various OSINT techniques can be exploited to gain useful intelligence from public sources about target computerized systems.

Technical Investigation of Target website

By knowing the type of programming language, web frameworks, content management system (CMS) used to create the target website, we can search for vulnerabilities that target these components (especially zero-day vulnerabilities) and then work to exploit any of these vulnerabilities instantly, once discovered.

There are different online services to examine the type of technology used to build websites. To use such service, all you need to do is to supply a target domain name, to have a full list of technical specifications and online libraries/programming languages used to build a subject website. These services also reveal the hosting provider of the target website, SSL certificate register name in addition to email system type. The following are some popular services to use:

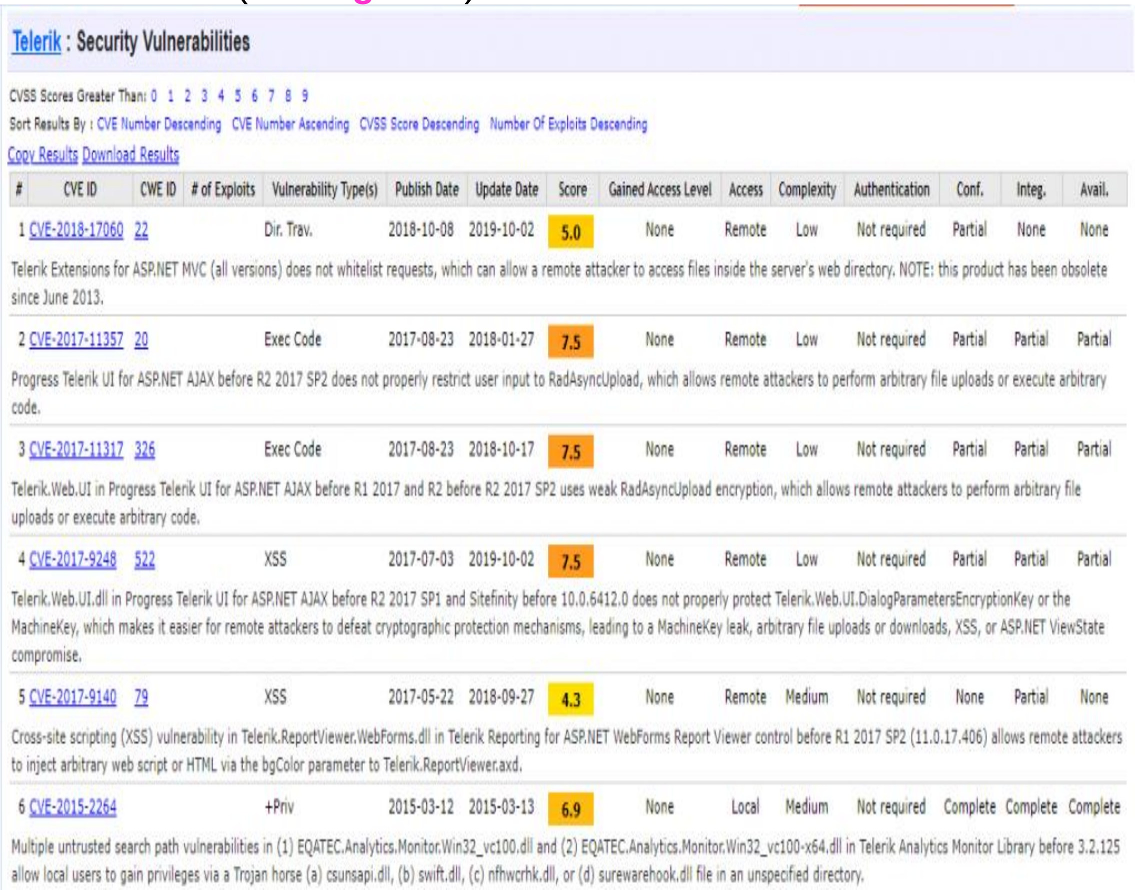
1. **https://builtwith.com**
2. **https://www.wappalyzer.com**

In the following screen capture, I use built *with* service to investigate the technical specifications of a target website. This reveals different technical information (see Figure 1) and opens the door to more examination for each technology used to build the subject website. Now, I need to check the list of technical specifications to see if there is unpatched operating systems or outdated content management system with known vulnerabilities that I can exploit to gain entrance to target system.

	Frameworks			
	ASP.NET 4.0	Nov 2013	Dec 2019	
	ASP.NET Programming Language	Jul 2012	Dec 2019	
	ASP.NET MVC	Feb 2017	Dec 2019	
	ASP.NET Ajax	Jul 2012	Feb 2017	⊘
	Content Delivery Network			
G	GStatic Google Static Content	Mar 2017	Nov 2019	
	Mobile			
G	Viewport Meta	Mar 2017	Dec 2019	
	IPhone / Mobile Compatible	Jun 2018	Dec 2019	
	Mapping			
G	Google Maps for Work	Dec 2017	Dec 2019	$
G	Google Maps API	Dec 2017	Dec 2019	
G	Google Maps Maps	Dec 2017	Dec 2019	
	JavaScript Libraries and Functions			
	jQuery JavaScript Library	Jul 2012	Dec 2019	
	Modernizr 2.6	Feb 2017	Dec 2019	
	jQuery UI jQuery Plugin - UI	Mar 2017	Dec 2019	
	Modernizr Compatibility	Mar 2017	Dec 2019	

Figure 1 – Using built with to investigate technology used to build the target website

For example, large numbers of ASP.net websites, use *Telerik Controls* (**https://www.telerik.com**) to enrich their design. To find security vulnerabilities associated with *Telerik Controls*, you can go to **https://www.cvedetails.com** and search for *Telerik* security vulnerabilities (see **Figure 2**).



Telerik : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-17060	22		Dir. Trav.	2018-10-08	2019-10-02	5.0	None	Remote	Low	Not required	Partial	None	None
Telerik Extensions for ASP.NET MVC (all versions) does not whitelist requests, which can allow a remote attacker to access files inside the server's web directory. NOTE: this product has been obsolete since June 2013.														
2	CVE-2017-11357	20		Exec Code	2017-08-23	2018-01-27	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Progress Telerik UI for ASP.NET AJAX before R2 2017 SP2 does not properly restrict user input to RadAsyncUpload, which allows remote attackers to perform arbitrary file uploads or execute arbitrary code.														
3	CVE-2017-11317	326		Exec Code	2017-08-23	2018-10-17	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Telerik.Web.UI in Progress Telerik UI for ASP.NET AJAX before R1 2017 and R2 before R2 2017 SP2 uses weak RadAsyncUpload encryption, which allows remote attackers to perform arbitrary file uploads or execute arbitrary code.														
4	CVE-2017-9248	522		XSS	2017-07-03	2019-10-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Telerik.Web.UI.dll in Progress Telerik UI for ASP.NET AJAX before R2 2017 SP1 and Sitefinity before 10.0.6412.0 does not properly protect Telerik.Web.UI.DialogParametersEncryptionKey or the MachineKey, which makes it easier for remote attackers to defeat cryptographic protection mechanisms, leading to a MachineKey leak, arbitrary file uploads or downloads, XSS, or ASP.NET ViewState compromise.														
5	CVE-2017-9140	79		XSS	2017-05-22	2018-09-27	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in Telerik.ReportViewer.WebForms.dll in Telerik Reporting for ASP.NET WebForms Report Viewer control before R1 2017 SP2 (11.0.17.406) allows remote attackers to inject arbitrary web script or HTML via the bgColor parameter to Telerik.ReportViewer.axd.														
6	CVE-2015-2264			+Priv	2015-03-12	2015-03-13	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
Multiple untrusted search path vulnerabilities in (1) EQATEC.Analytics.Monitor.Win32_vc100.dll and (2) EQATEC.Analytics.Monitor.Win32_vc100-x64.dll in Telerik Analytics Monitor Library before 3.2.125 allow local users to gain privileges via a Trojan horse (a) csunsapi.dll, (b) swift.dll, (c) nfhwcrhk.dll, or (d) surewarehook.dll file in an unspecified directory.														

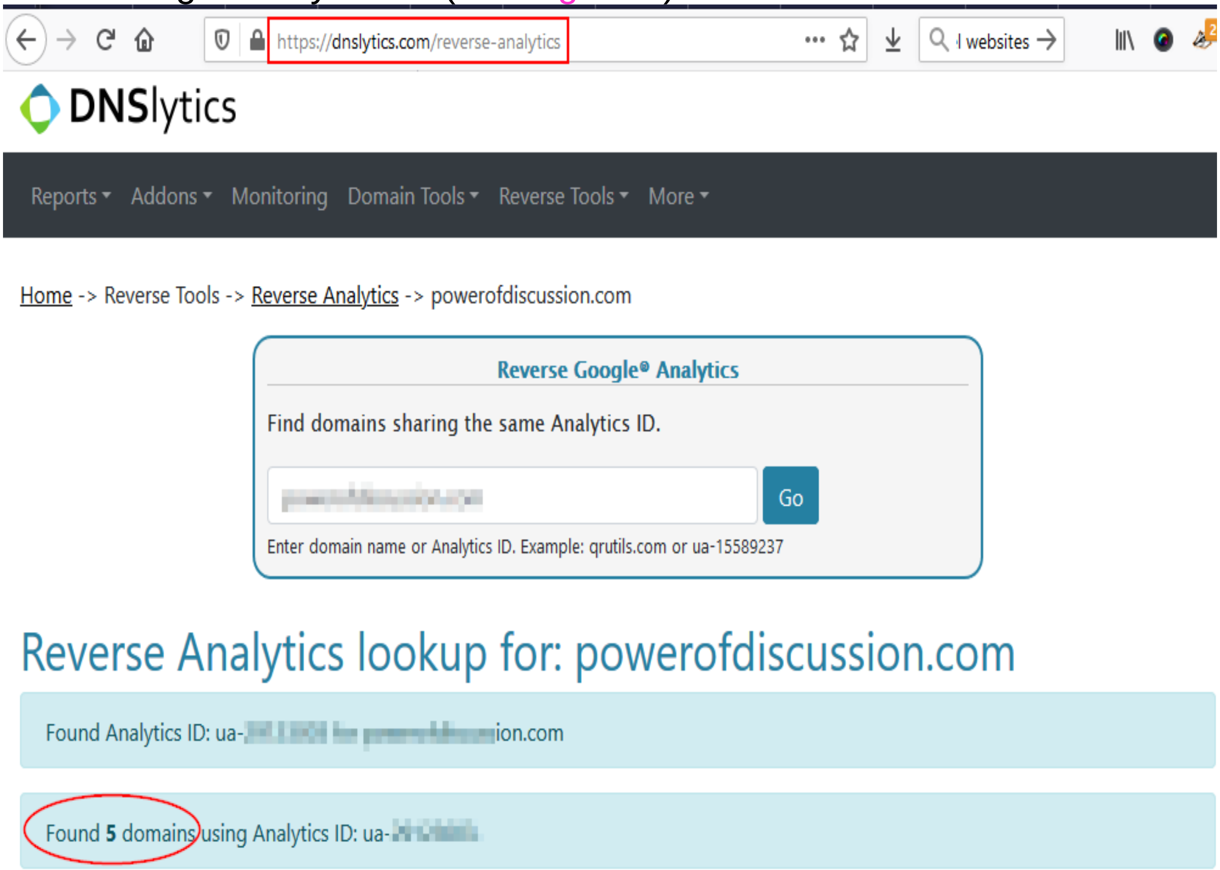
Figure 2 – List of security vulnerabilities for Telerik Controls

There are many websites that list security vulnerabilities of operating systems, software and other web applications. The following are the most popular one that we can use to search for common security vulnerabilities and exposures:

1. https://vulmon.com
2. https://sploitus.com
3. https://www.saucs.com
4. https://www.shodan.io

Analytics and Tracking

Most websites use Google services to analyze traffic and serve advertisements. We can use this feature to capture all linked domain names. For example, I can find all websites that use the same *Google AdSense* or *Analytical* accounts. *Dnslytics* (**https://dnslytics.com/reverse-analytics)** is a free online service that finds domains sharing the same Google Analytics ID (see Figure 3).



Home -> Reverse Tools -> Reverse Analytics -> powerofdiscussion.com

Reverse Google® Analytics

Find domains sharing the same Analytics ID.

[redacted]

Enter domain name or Analytics ID. Example: qrutils.com or ua-15589237

Reverse Analytics lookup for: powerofdiscussion.com

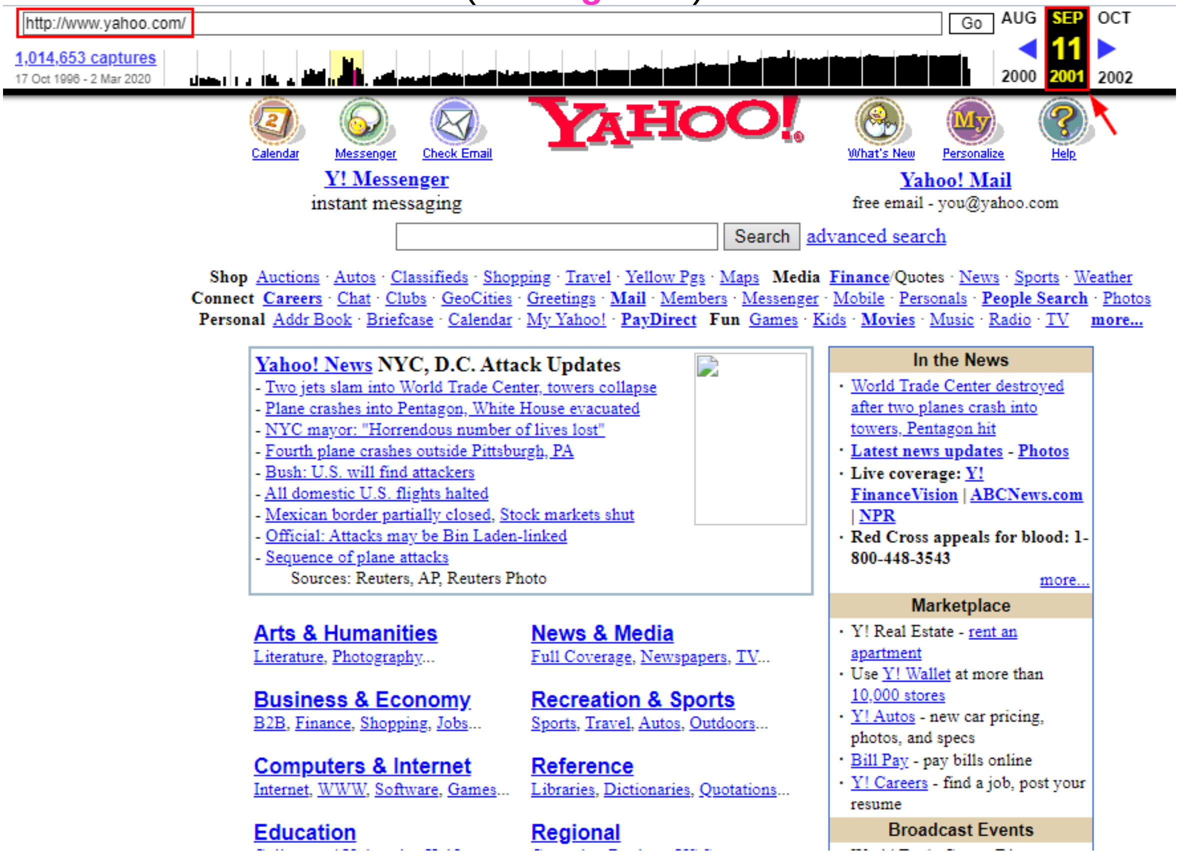
Found Analytics ID: ua-[redacted] for [redacted]ion.com

Found **5** domains using Analytics ID: ua-[redacted]

Figure 3 – Using reverse Google Analytics service to reveal domain names belong to the same entity

Target website previous History

In many instances, checking the old version of the target website can reveal important information. For example, an old website version of a corporation may reveal top managements' email addresses and phone numbers before they got removed from the new version. Wayback Machine (https://archive.org/web) is a good place to start your search for old versions of websites (see Figure 4).



Y! Messenger
instant messaging

Yahoo! Mail
free email - you@yahoo.com

advanced search

Shop Auctions · Autos · Classifieds · Shopping · Travel · Yellow Pgs · Maps **Media** Finance/Quotes · News · Sports · Weather
Connect Careers · Chat · Clubs · GeoCities · Greetings · Mail · Members · Messenger · Mobile · Personals · People Search · Photos
Personal Addr Book · Briefcase · Calendar · My Yahoo! · PayDirect **Fun** Games · Kids · Movies · Music · Radio · TV **more...**

Yahoo! News NYC, D.C. Attack Updates
- Two jets slam into World Trade Center, towers collapse
- Plane crashes into Pentagon, White House evacuated
- NYC mayor: "Horrendous number of lives lost"
- Fourth plane crashes outside Pittsburgh, PA
- Bush: U.S. will find attackers
- All domestic U.S. flights halted
- Mexican border partially closed, Stock markets shut
- Official: Attacks may be Bin Laden-linked
- Sequence of plane attacks

Sources: Reuters, AP, Reuters Photo

In the News
- World Trade Center destroyed after two planes crash into towers, Pentagon hit
- **Latest news updates** - **Photos**
- **Live coverage: Y! FinanceVision | ABCNews.com | NPR**
- **Red Cross appeals for blood: 1-800-448-3543**

more...

Arts & Humanities
Literature, Photography...

News & Media
Full Coverage, Newspapers, TV...

Business & Economy
B2B, Finance, Shopping, Jobs...

Recreation & Sports
Sports, Travel, Autos, Outdoors...

Computers & Internet
Internet, WWW, Software, Games...

Reference
Libraries, Dictionaries, Quotations...

Education

Regional

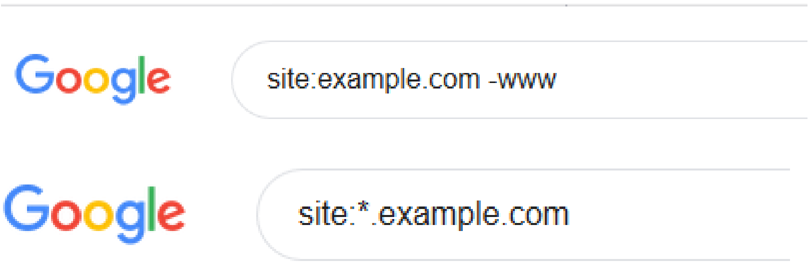
Marketplace
- Y! Real Estate - rent an apartment
- Use Y! Wallet at more than 10,000 stores
- Y! Autos - new car pricing, photos, and specs
- Bill Pay - pay bills online
- Y! Careers - find a job, post your resume

Broadcast Events

Figure 4 -Using the Wayback machine to see previous versions of websites

Sub-domain name Discovery

Finding a target website sub-domains is important and can reveal sensitive information about the target such as the VPN portal, email system and FTP server address where some files may have left unprotected. To find all sub-domain names of a target indexed by Google, use the following Google search command (see Figure 5).



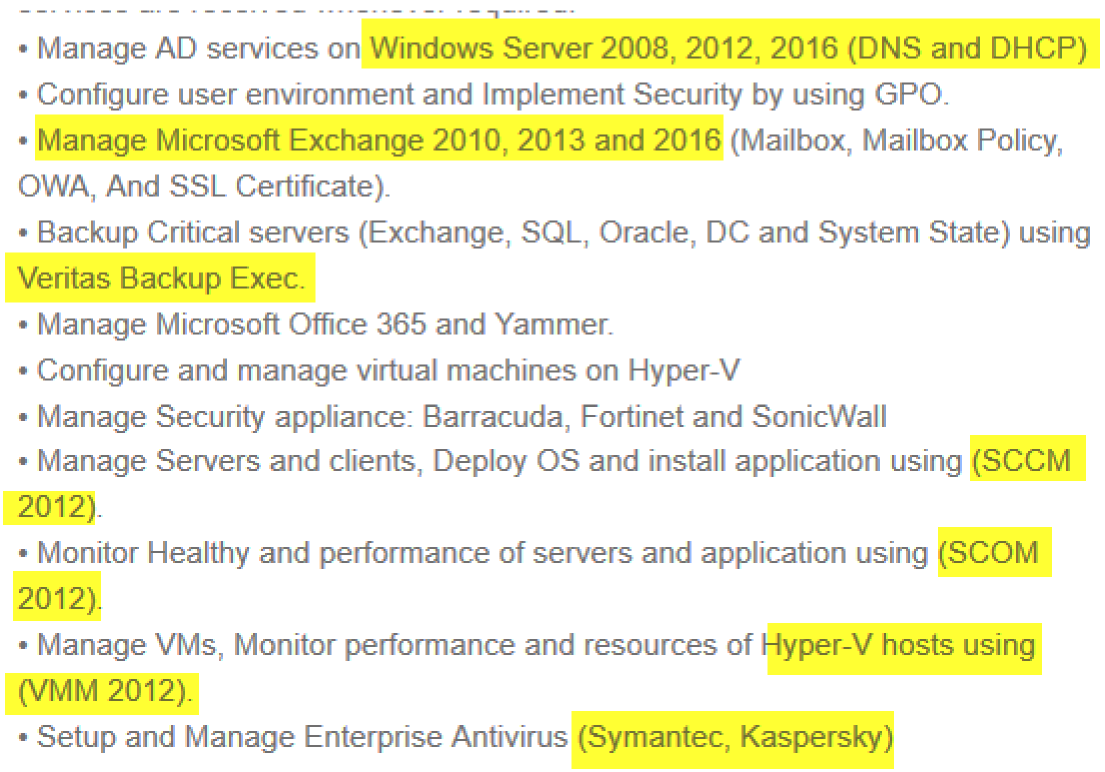
```
site:example.com -www
```

```
site:*.example.com
```

Figure 5 – Replace example.com with your target domain name

Type and versions of IT infrastructure of the target company

Job websites – and any job announcement posted on the target website – should be analyzed to discover the exact IT infrastructure used by the target organization. For example, I conducted a simple search on employee resumes on job websites and was able to capture important information about target organization security systems (e.g. Firewalls and Intrusion Detection Systems), server operating system type, email system, networking devices, types of backup systems and much more (see Figure 6).



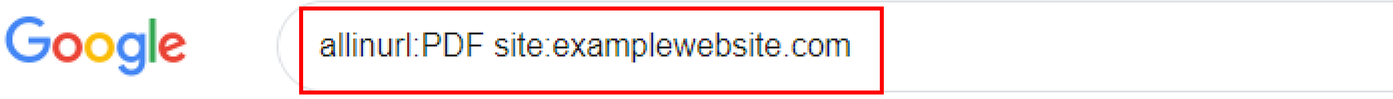
- Manage AD services on Windows Server 2008, 2012, 2016 (DNS and DHCP)
- Configure user environment and Implement Security by using GPO.
- Manage Microsoft Exchange 2010, 2013 and 2016 (Mailbox, Mailbox Policy, OWA, And SSL Certificate).
- Backup Critical servers (Exchange, SQL, Oracle, DC and System State) using Veritas Backup Exec.
- Manage Microsoft Office 365 and Yammer.
- Configure and manage virtual machines on Hyper-V
- Manage Security appliance: Barracuda, Fortinet and SonicWall
- Manage Servers and clients, Deploy OS and install application using (SCCM 2012).
- Monitor Healthy and performance of servers and application using (SCOM 2012).
- Manage VMs, Monitor performance and resources of Hyper-V hosts using (VMM 2012).
- Setup and Manage Enterprise Antivirus (Symantec, Kaspersky)

Figure 6 – Sample resume found on a job website that reveals the type of IT infrastructure of the target organization

Harvest digital files hosted on the target domain name

Using advanced Google search engine techniques (also known as Google dorks) can reveal a great amount of information about the target organizations' IT systems in addition to confidential files left on the public server. There are thousands of Google dorks and you can practice creating yours. A comprehensive list of Google dorks can be found in the Google Hacking **Database (https://www.exploit-db.com/google-hacking-database).**

I will experiment using Google dork to locate all PDF files posted on the target website (see **Figure 7**):



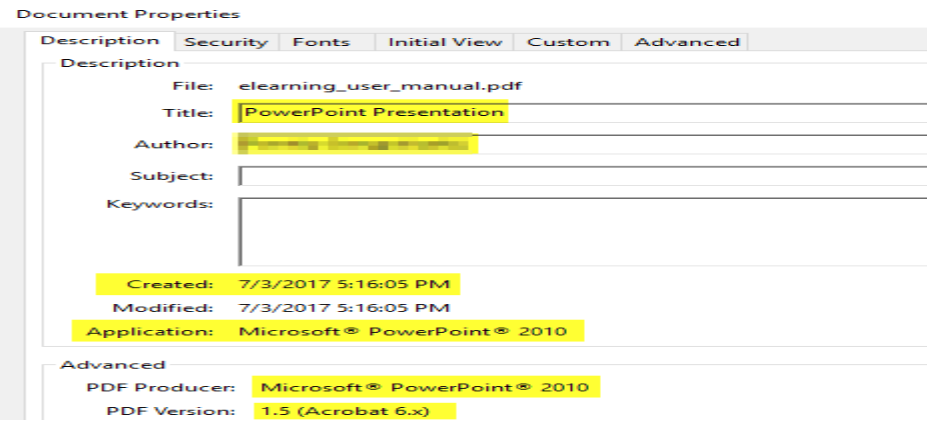
```
allinurl:PDF site:examplewebsite.com
```

Figure 7 – Find all PDF files on the target domain name

In the above example, I searched for PDF files, however, you can change the file type to something else as you want (doc, docx, xls, txt).

Information contained within files metadata

For each file found on the target website, we should investigate its metadata. Metadata is data about data. In technical terms, it contains hidden descriptive information about the file it belongs to. For example, some metadata included in an MS Office document file might include the author's name, date/time created, comments, software used to create the file in addition to the type of OS of the device used to create this file. (see **Figure 8**).



Description

File: elearning_user_manual.pdf

Title: PowerPoint Presentation

Author: [redacted]

Subject:

Keywords:

Created: 7/3/2017 5:16:05 PM

Modified: 7/3/2017 5:16:05 PM

Application: Microsoft® PowerPoint® 2010

Advanced

PDF Producer: Microsoft® PowerPoint® 2010

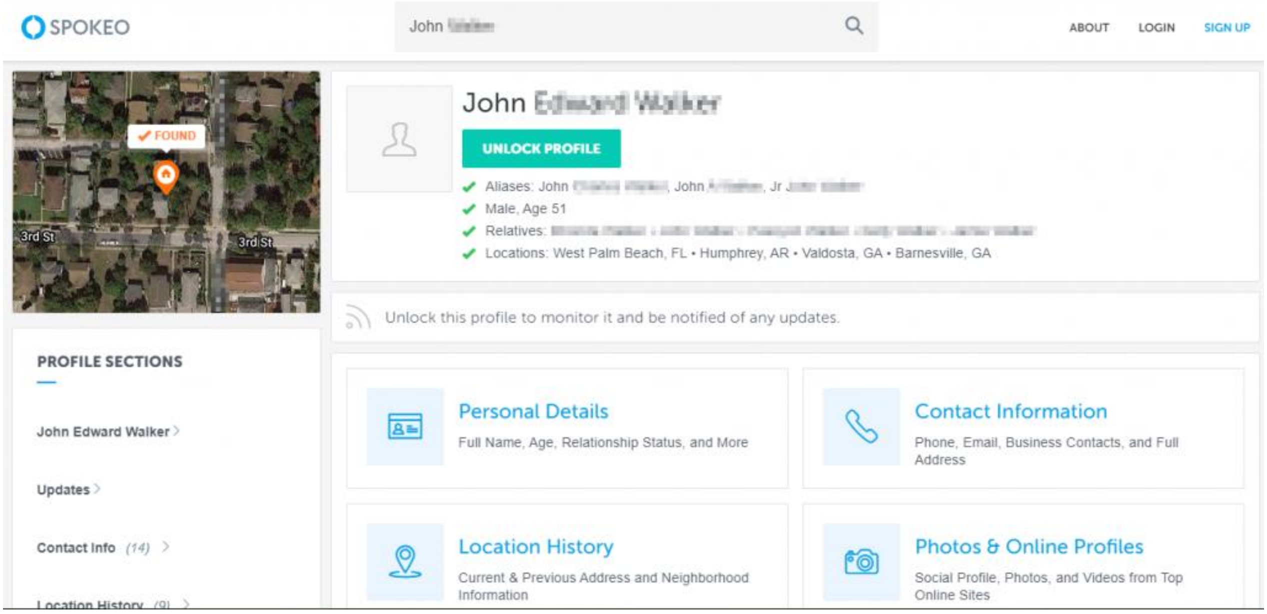
PDF Version: 1.5 (Acrobat 6.x)

Figure 8 – Checking a PDF file metadata info

From Figure 8, I found the following facts about the subject PDF file metadata:

1. Installed PDF reader Version on the creation device: **1.5**
2. Application used to create the report: **MS PowerPoint 2010** (using the “Save As” function)
3. Type of OS used on the target device: **Windows**
4. File creation date/time: **July 2017**
5. **Author Name** (The person who creates the file).
   If the file contains an author name, an additional search could be conducted to lock up more details of the file’s author using specialized people data collection websites. The following lists some popular people search engines:

1. **Spokeo (https://www.spokeo.com) (see Figure 9)**
2. **Truepeoplesearch (https://www.truepeoplesearch.com)**
3. **Truthfinder (https://www.truthfinder.com)**
4. **411 (https://www.411.com**)



SPOKEO

John [redacted]

ABOUT LOGIN SIGN UP

✓ FOUND

3rd St

3rd St

John [redacted]

UNLOCK PROFILE

✓ Aliases: John [redacted], John [redacted], Jr [redacted]
✓ Male, Age 51
✓ Relatives: [redacted]
✓ Locations: West Palm Beach, FL • Humphrey, AR • Valdosta, GA • Barnesville, GA

Unlock this profile to monitor it and be notified of any updates.

PROFILE SECTIONS

John Edward Walker >

Updates >

Contact Info (14) >

Location History (9) >

Personal Details
Full Name, Age, Relationship Status, and More

Contact Information
Phone, Email, Business Contacts, and Full Address

Location History
Current & Previous Address and Neighborhood Information

Photos & Online Profiles
Social Profile, Photos, and Videos from Top Online Sites

Figure 9 – Using SPOKEO to lock up information about people you know

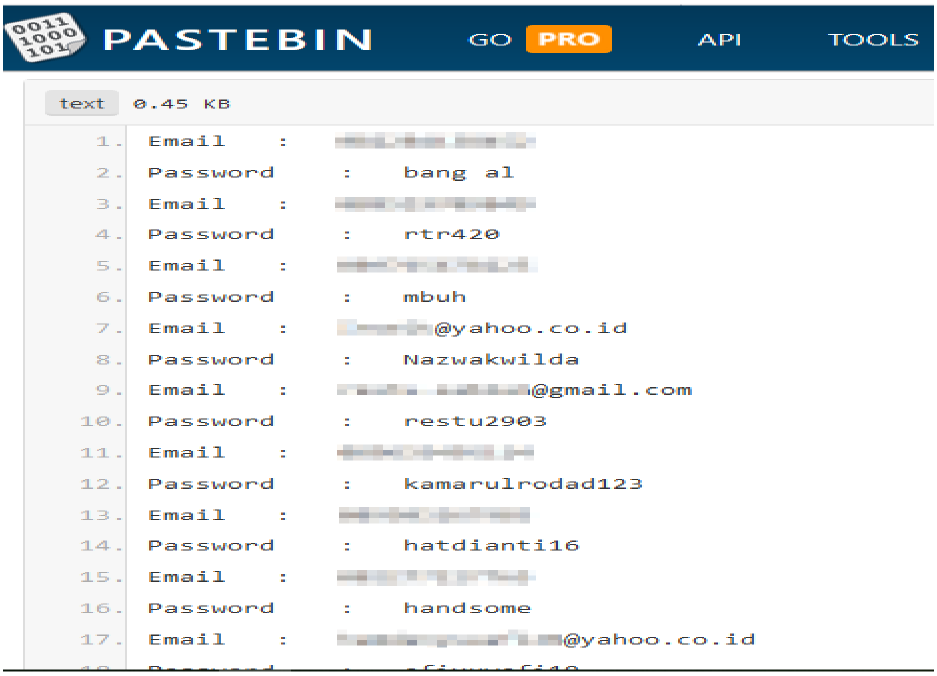
Email naming criteria

To predicate the naming criteria used by the target organization when creating new email accounts, we should investigate the naming of current email addresses. For example, many organizations use the following naming criteria:

- Most common patterns of naming new emails: **{first}(DOT){last first three characters}@exampleWebsite.com**
- Other naming criteria include: **{first}@exampleWebsite.com**
  I usually use this website **https://www.email-format.com** to find the email address formats in use at thousands of companies.

Leaked Credentials

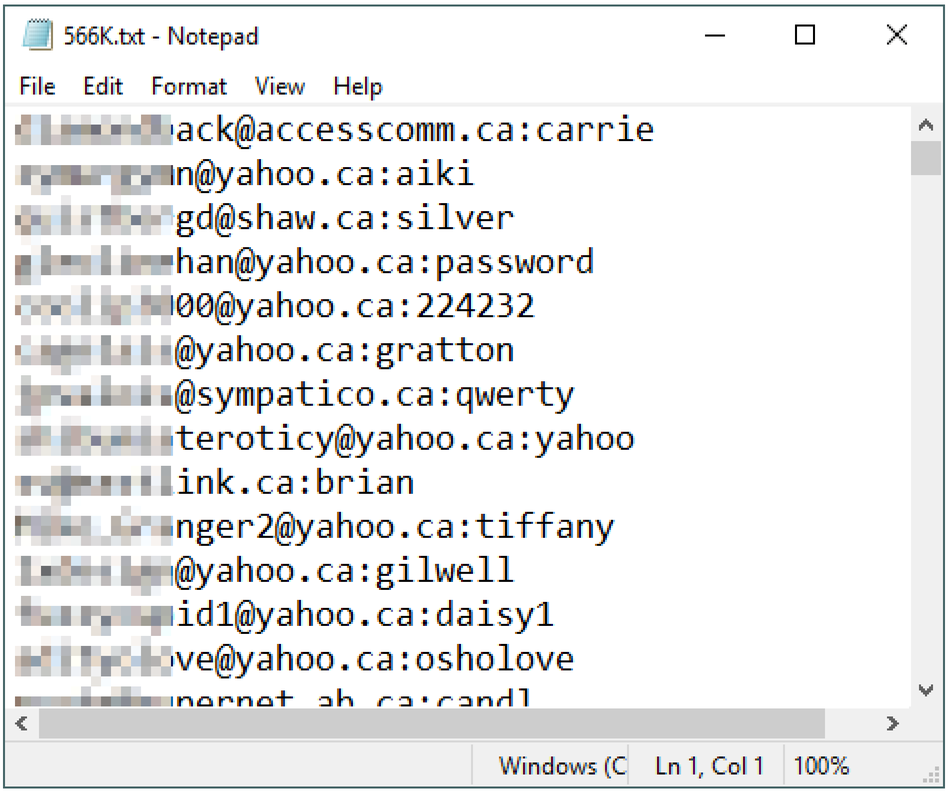
Leaked accounts credentials are spread everywhere online, especially in the darknet. For example, pastebin websites (**see Figure 10**) contain a vast amount of leaked credentials.



```
Email    :   [redacted]
Password      :    bang al
Email    :   [redacted]
Password      :    rtr420
Email    :   [redacted]
Password      :    mbuh
Email    :   [redacted]@yahoo.co.id
Password      :    Nazwakwilda
Email    :   [redacted]@gmail.com
Password      :    restu2903
Email    :   [redacted]
Password      :    kamarulrodad123
Email    :   [redacted]
Password      :    hatdianti16
Email    :   [redacted]
Password      :    handsome
Email    :   [redacted]@yahoo.co.id
```

Figure 10 – Leaked credentials found on Pastebin.com

Anonymous file sharing websites, such as **https://anonfile.com** (see **Figure 11**) also contain large numbers of leaked credential files with billions of records



```
[redacted]ack@accesscomm.ca:carrie
[redacted]n@yahoo.ca:aiki
[redacted]gd@shaw.ca:silver
[redacted]han@yahoo.ca:password
[redacted]00@yahoo.ca:224232
[redacted]@yahoo.ca:gratton
[redacted]@sympatico.ca:qwerty
[redacted]teroticy@yahoo.ca:yahoo
[redacted]ink.ca:brian
[redacted]nger2@yahoo.ca:tiffany
[redacted]@yahoo.ca:gilwell
[redacted]id1@yahoo.ca:daisy1
[redacted]ve@yahoo.ca:osholove
[redacted]nernet.ab.ca:candl
```

Figure 11 – A file hosted on https://anonfile.com contains thousands of leaked credentials

Conclusion

In this article, I tried to give a brief overview of OSINT capabilities and how to use it to gather useful intelligence about different entities.

In today's information age, having OSINT skills is something great to have, however, there are many things – or prerequisites – you should master in order to make your OSINT search rich and effective. For instance, before you begin your OSINT search, you should learn how to conceal your digital identity and become anonymous online. This is essential to prevent threat actors from discovering your search activities. OSINT is strongly related to Digital Forensics and knowing basic information about digital forensics operations will also prove useful when conducting OSINT gathering activities.

3. Discuss the legal and ethical considerations involved in conducting network scanning and enumeration during ethical hacking activities

Since the early days of computing, ethical hackers have used enumeration to access systems and networks. Enumeration is the process of systematically probing a target for information, and it remains an essential tool in the hacker's arsenal. Enumeration can provide attackers with a roadmap to entering a system by identifying open ports, usernames, and passwords.

While many commercial tools are available for enumeration, knowing how to use basic command-line tools can be just as effective. some of the most common enumeration techniques and discuss how they can be used in ethical hacking.

"Knowing your enemy is winning half the war"

Similarly, when you know about your target, half the task of Hacking is done. There are different ways to gather information about your target.

Network Scanning

Network Scanning is the procedure of identifying active hosts, ports and the services used by the target application. Suppose you are an Ethical Hacker and want to find vulnerabilities in the System, you need a point in the System that you can try to attack. Network Scanning for Ethical Hacking is used to find out these points in the system that a Black Hat Hacker can use to hack the network. And then the respective teams work on improving the security of the network. If you are excited to know more about Ethical hacking, join the Ethical Hacking Course Online today.

Every Organization has a Network. This network could be an internal network which consists of all the systems connected with each other, or it can be a network that's connected to the internet. In either case, to hack the network, you will have to find a vulnerable point in the network that can be exploited. Network Scanning is used to find out such points in the network.

How is Network Scanning different from Reconnaissance?

Think of it like this: You are an army officer and you and your team are planning to attack a terrorist lair. You have found out the location of the lair and details about the surroundings and also found ways to send the team to the lair. You can consider all this as the information you've gathered using Reconnaissance. Now you have to find a point through which you can enter the lair and attack the enemy. This is **Network Scanning**.

In simple terms, Reconnaissance is used to gather information and understand your target, and Network Scanning is a method used to find possible vulnerable points in the network through which you can hack the network.
Depending on what kind of information the Scan identifies, Network Scanning can be classified into different types.

Types of Network Scanning for Ethical Hacking

Network Scanning can be classified into two main categories:

1. **Port Scanning**
2. **Vulnerability Scanning**

Port Scanning

As the name suggests, Port Scanning is a process used to find out active ports on the network. A Port Scanner sends client requests to the range of ports on the target network and then saves the details about the ports that send a response back. This is how active ports are found.

There are different types of Port Scanning. Below is a list of some of the most used ones:

- TCP scanning
- SYN scanning
- UDP scanning
- ACK scanning
- Window scanning
- FIN scanning

Vulnerability Scanning

Vulnerability Scanning is a type of Network Scanning for Ethical Hacking used to find out weaknesses in the network. This type of scanning identifies vulnerabilities that occur due to poor programming or misconfiguration of the network.

Now that you know what Network Scanning is, I will introduce you to some tools and tell you how to use them for Network Scanning.

How to use Network Scanning tools?

In this section of Network Scanning for Ethical Hacking blog, I will show you how to use some Network Scanning tools. The Operating System I am using for this is Kali Linux because it comes with many in-built tools for Hacking.

The first tool I am going to talk about is Nmap.

1. Nmap for Network Scanning

Nmap is a free and open source network scanner. You can scan a network with Nmap either by using the IP address of the target:

```
$ nmap 1.2.3.4
```

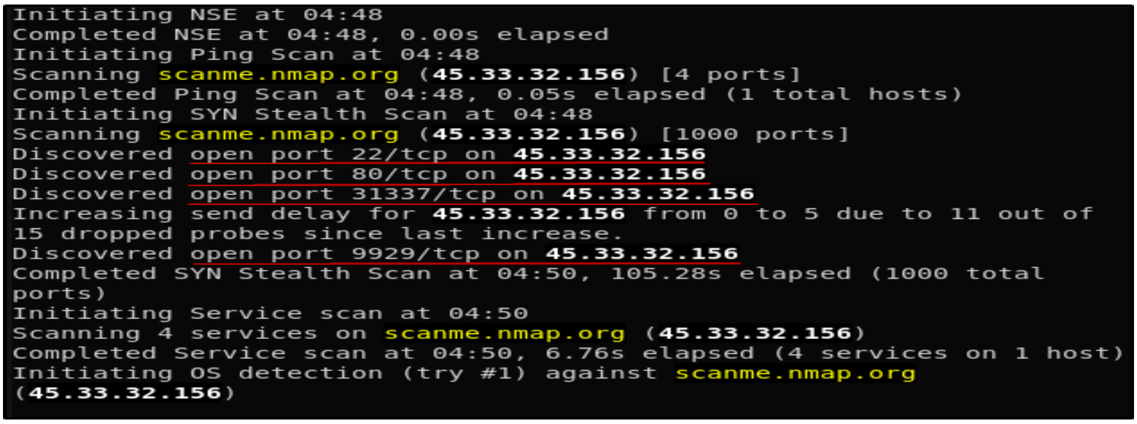
Or using the hostname

```
$ nmap example.com
```

Note that it is illegal to scan the network of any organization without prior authorization by the organization. So don't try to scan just any random network. But if we can't scan any network without permission, then how will we learn about Nmap? Don't worry, the Nmap Organization has provided a website for us to practice scanning using Nmap: scanme.nmap.org

Let's try scanning this. Open a terminal in your system and run the below command:

```
$ Nmap -v -A scanme.nmap.org
```



```
Initiating NSE at 04:48
Completed NSE at 04:48, 0.00s elapsed
Initiating Ping Scan at 04:48
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 04:48, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 04:48
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 11 out of
15 dropped probes since last increase.
Discovered open port 9929/tcp on 45.33.32.156
Completed SYN Stealth Scan at 04:50, 105.28s elapsed (1000 total
ports)
Initiating Service scan at 04:50
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 04:50, 6.76s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org
(45.33.32.156)
```

You can see how Nmap displays the open ports on the network in the result. In the above command, option ‘**v**‘ is for verbose output and option ‘**A**‘ is to detect the Operating System.

There are a lot of options that can be used with the Nmap tool to obtain different kinds of results. To understand more about using the Nmap tool, check out this Nmap tutorial.

Legal Issues

When used properly, Nmap helps protect your network from invaders. But when used improperly, Nmap can (in rare cases) get you sued, fired, expelled, jailed, or banned by your ISP. Reduce your risk by reading this legal guide before launching Nmap.

Is Unauthorized Port Scanning a Crime?

The legal ramifications of scanning networks with Nmap are complex and so controversial that third-party organizations have even printed T-shirts and bumper stickers promulgating opinions on the matter, as shown in Figure 1.3. The topic also draws many passionate but often unproductive debates and flame wars. If you ever participate in such discussions, try to avoid the overused and ill-fitting analogies to knocking on someone's home door or testing whether his door and windows are locked.

Figure shows Strong opinions on port scanning legality and morality

While I agree with the sentiment that port scanning *should not* be illegal, it is rarely wise to take legal advice from a T-shirt. Indeed, taking it from a software engineer and author is only slightly better. Speak to a competent lawyer within your jurisdiction for a better understanding of how the law applies to your particular situation. With that important disclaimer out of the way, I'll provide some general information that may prove helpful.

The best way to avoid controversy when using Nmap is to always secure written authorization from the target network representatives before initiating any scanning. There is still a chance that your ISP will give you trouble if they notice it (or if the target administrators accidentally send them an abuse report), but this is usually easy to resolve. When you are performing a penetration test, this authorization should be in the Statement of Work. When testing your own company, make certain that this activity clearly falls within your job description. Security consultants should be familiar with the excellent Open Source Security Testing Methodology Manual (OSSTMM), which provides best practices for these situations.

While civil and (especially) criminal court cases are the nightmare scenario for Nmap users, these are very rare. After all, no United States federal laws explicitly criminalize port scanning. A much more frequent occurrence is that the target network will notice a scan and send a complaint to the network service provider where the scan initiated (your ISP). Most network administrators do not seem to care or notice the many scans bouncing off their networks daily, but a few complain. The scan source ISP may track down the user corresponding to the reported IP address and time, then chide the user or even kick him off the service. Port scanning without authorization is sometimes against the provider's acceptable use policy (AUP). For example, the AUP for the huge cable-modem ISP Comcast says:

Network probing or port scanning tools are only permitted when used in conjunction with a residential home network, or if explicitly authorized by the destination host and/or network. Unauthorized port scanning, for any reason, is strictly prohibited.

Even if an ISP does not explicitly ban unauthorized port scanning, they might claim that some “anti-hacking” provision applies. Of course this does *not* make port scanning illegal. Many perfectly legal and (in the United States) constitutionally protected activities are banned by ISPs. For example, the AUP quoted above also prohibits users from transmitting, storing, or posting “any information or material which a reasonable person could deem to be objectionable, offensive, indecent, pornographic, embarrassing, distressing, vulgar, hateful, racially or ethnically offensive, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful”. In other words, some ISPs ban any behaviour that could possibly offend or annoy someone. Indiscriminate scanning of other people's networks does have that potential. If you decide to perform such controversial scanning anyway, never do it from work, school, or any other service provider that has substantial control over your well-being. Use a commercial broadband or wireless provider instead. Losing your DSL connection and having to change providers is a slight nuisance, but it is immeasurably preferable to being expelled or fired.

While legal cases involving port scanning (without follow-up hacking attacks) are rare, they do happen. One of the most notable cases involved a man named Scott Moulton who had an ongoing consulting contract to maintain the Cherokee County, Georgia emergency 911 system. In December 1999, he was tasked with setting up a router connecting the Canton, Georgia Police Department with the E911 Center. Concerned that this might jeopardize the E911 Center security, Scott initiated some preliminary port scanning of the networks involved. In the process he scanned a Cherokee County web server that was owned and maintained by a competing consulting firm named VC3. They noticed the scan and emailed Scott, who replied that he worked for the 911 Center and was testing security. VC3 then reported the activity to the police. Scott lost his E911 maintenance contract and was arrested for allegedly violating the Computer Fraud and Abuse Act of America Section 1030(a) (5)(B). This act applies against anyone who “intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage” (and meets other requirements). The damage claimed by VC3 involved time spent investigating the port scan and related activity. Scott sued VC3 for defamation, and VC3 countersued for violation of the Computer Fraud and Abuse Act as well as the Georgia Computer Systems Protection Act.

The civil case against Scott was dismissed before trial, implying a complete lack of merit. The ruling made many Nmap users smile:

“Court holds that plaintiff's act of conducting an unauthorized port scan and throughput test of defendant's servers does not constitute a violation of either the Georgia Computer Systems Protection Act or the Computer

Fraud and Abuse Act.”—Civ. Act. No. 1:00-CV-434-TWT (N.D. Ga. November 6, 2000)

This was an exciting victory in the civil case, but Scott still had the criminal charges pending. Fortunately he kept his spirits high, sending the following note to the *nmap-hackers* mailing list:

I am proud that I could be of some benefit to the computer society in defending and protecting the rights of specialists in the computer field, however it is EXTREMELY costly to support such an effort, of which I am not happy about. But I will continue to fight and prove that there is nothing illegal about port scanning especially when I was just doing my job.

Eventually, the criminal court came to the same conclusion and all charges were dropped. While Scott was vindicated in the end, he suffered six-figure legal bills and endured stressful years battling through the court system. The silver lining is that after spending so much time educating his lawyers about the technical issues involved, Scott started a successful forensics services company.

While the Moulton case sets a good example (if not legal precedent), different courts or situations could still lead to worse outcomes. Remember that many states have their own computer abuse laws, some of which can arguably make even pinging a remote machine without authorization illegal.

Laws in other nations obviously differ as well. For example, A 17-year-old youth was convicted in Finland of attempted computer intrusion for simply port scanning a bank. He was fined to cover the target's investigation expenses. The Moulton ruling might have differed if the VC3 machine had actually crashed and they were able to justify the $5,000 damage figure required by the act.

At the other extreme, an Israeli judge acquitted Avi Mizrahi in early 2004 for vulnerability scanning the Mossad secret service. Judge Abraham Tennenbaum even commended Avi in his ruling:

In a way, Internet surfers who check the vulnerabilities of Web sites are acting in the public good. If their intentions are not malicious and they do not cause any damage, they should even be praised.

In 2007 and 2008, broad new cybercrime laws took effect in Germany and England. These laws are meant to ban the distribution, use, and even possession of “hacking tools”. For example, the UK amendment to the Computer Misuse Act makes it illegal to “supply or offer to supply [a program], believing that it is likely to be used to commit, or to assist in the commission of [a Computer Misuse Act violation]”. These laws have already led some security tool authors to close shop or move their projects to other countries. The problem is that most security tools can be used by both ethical professionals (white-hats) to defend their networks and black-hats to attack. These dangerous laws are based on the tool author or user's intent, which is subjective and hard to divine. Nmap was designed to help secure the Internet, but I'd hate to be arrested and forced to defend my intentions to a judge and jury, especially in a foreign country like Germany where I don't even speak the language. These laws are unlikely to affect tools as widespread and popular as Nmap, but they have had a chilling effect on smaller tools and those which are more commonly abused by computer criminals (such as exploitation frameworks).

Regardless of the legal status of port scanning, ISP accounts will continue to be terminated if many complaints are generated. The best way to avoid ISP abuse reports or civil/criminal charges is to avoid annoying the target network administrators in the first place. Here are some practical suggestions:

- Ensure that you have permission to scan. Probably at least 90% of network scanning is non-controversial. You are rarely badgered for scanning your own machine or the networks you administer. The controversy comes when scanning other networks. There are many reasons (good and bad) for doing this sort of network exploration. Perhaps you are scanning the other systems in your dorm or department to look for publicly shared files (FTP, SMB, WWW, etc.). Or maybe you are just trying to find the IP address of a certain printer. You might have scanned your favorite web site to see if they are offering any other services, or because you were curious what OS they run. Perhaps you are just trying to test connectivity, or maybe you wanted to do a quick security sanity check before handing off your credit card details to that e-commerce company. You might be conducting Internet research. Or are you performing initial reconnaissance in preparation for a break-in attempt? The remote administrators rarely know your true intentions, and do sometimes get suspicious. The best approach is to get permission first. I have seen a few people with non-administrative roles land in hot water after deciding to “prove” network insecurity by launching an intrusive scan of the entire company or campus. Administrators tend to be more cooperative when asked in advance than when woken up at 3:00 AM by an IDS alarm claiming they are under massive attack. So whenever possible, obtain written authorization before scanning a network. Adrian Lamo would probably have avoided jail if he had asked the New York Times to test their security rather than telling reporters about the flaws afterward. Unfortunately they might have said no. Be prepared for this answer.

- Target your scan as tightly as possible. Any machine connected to the Internet is scanned regularly enough that most administrators ignore such Internet background noise. But scanning enough networks or executing very noisy/intrusive scans increases the probability of generating complaints. So if you are only looking for web servers, specify -p80 rather than scanning all 65,536 TCP ports on each machine. If you are only trying to find available hosts, do an Nmap ping scan rather than full port scan. Do not scan a CIDR /16 (65K hosts) when a /24 netblock suffices. The random scan mode now takes an argument specifying the number of hosts, rather than running forever. So consider -iR 1000 rather than -iR 10000 if the former is sufficient. Use the default timing (or even -T polite) rather than -T insane. Avoid noisy and relatively intrusive scans such as version detection (-sV) or NSE (--script). Similarly, a SYN scan (-sS) is quieter than a connect scan (-sT) while providing the same information and often being faster.
- As noted previously, do not do anything controversial from your work or school connections. Even though your intentions may be good, you have too much to lose if someone in power (e.g. boss, dean) decides you are a malicious cracker. Do you really want to explain your actions to someone who may not even know what port scanning means? Spend $40 a month for a shell, cell data, or residential broadband account. Not only are the repercussions less severe if you offend someone from such an account, but target network administrators are less likely to even bother complaining to mass-market providers. Also read the relevant AUP and choose a provider accordingly. If your provider (like Comcast discussed above) bans any unauthorized port scanning and posting of “offensive” material, do not be surprised if you are kicked off for this activity. In general, the more you pay to a service provider the more accommodating they are. A T1 provider is highly unlikely to yank your connection without notice because someone reported being port scanned. A dialup or residential DSL/cable provider very well might. This can happen even when the scan was forged by someone else.

- Nmap offers many options for stealthy scans, including source-IP spoofing, decoy scanning, and the more recent idle scan technique. These are discussed in the IDS evasion chapter. But remember that there is always a trade-off. You are harder to find if you launch scans from an open WAP far from your house, with 17 decoys, while doing subsequent probes through a chain of nine open proxies. But if anyone does track you down, they will be mighty suspicious of your intentions.
- Always have a legitimate reason for performing scans. An offended administrator might write to you first (or your ISP might forward his complaint to you) expecting some sort of justification for the activity. In the Scott Moulton case discussed above, VC3 first emailed Scott to ask what was going on. If they had been satisfied with his answer, matters might have stopped there rather than escalating into civil and criminal litigation. When I scan large portions of the Internet for research purposes, I use a reverse-DNS name that describes the project and run a web server on that IP address with detailed information and opt-out instructions.

Also remember that ancillary and subsequent actions are often used as evidence of intent. A port scan by itself does not always signify an attack. A port scan followed closely by an IIS exploit, however, broadcasts the intention loud and clear. This is important because decisions to prosecute (or fire, expel, complain, etc.) are often based on the whole event and not just one component (such as a port scan).

One dramatic case involved a Canadian man named Walter Nowakowski, who was apparently the first person to be charged in Canada with theft of communications (Canadian Criminal Code Section S.342.1) for accessing the Internet through someone's unsecured Wi-Fi network. Thousands of Canadian “war drivers” do this every day, so why was he singled out? Because of ancillary actions and intent. He was allegedly caught driving the wrong way on a one-way street, naked from the waist down, with laptop in hand, while downloading child pornography through the aforementioned unsecured wireless access point. The police apparently considered his activity egregious enough that they brainstormed for relevant charges and tacked on theft of communications to the many child pornography-related charges.

Similarly, charges involving port scanning are usually reserved for the most egregious cases. Even when paranoid administrators notify the police that they have been scanned, prosecution (or any further action) is exceedingly rare. The fact that a 911 emergency service was involved is likely what motivated prosecutors in the Moulton case. Your author scanned millions of Internet hosts while writing this book and received fewer than ten complaints.

To summarize this whole section, the question of whether port scanning is legal does not have a simple answer. I cannot unequivocally say “port scanning is never a crime”, as much as I would like to. Laws differ dramatically between jurisdictions, and cases hinge on their particular details. Even when facts are nearly identical, different judges and prosecutors do not always interpret them the same way. I can only urge caution and reiterate the suggestions above.

For testing purposes, you have permission to scan the host scanme.nmap.org. You may have noticed it used in several examples already. Note that this permission only includes scanning with Nmap and not testing exploits or denial of service attacks. To conserve bandwidth, please do not initiate more than a dozen scans against that host per day. If this free scanning target service is abused, it will be taken down and Nmap will report Failed to resolve given hostname/IP: scanme.nmap.org.

Can Port Scanning Crash the Target Computer/Networks?

Nmap does not have any features designed to crash target networks. It usually tries to tread lightly. For example, Nmap detects dropped packets and slows down when they occur in order to avoid overloading the network. Nmap also does not send any corrupt packets. The IP, TCP, UDP, and ICMP headers are always appropriate, though the destination host is not necessarily expecting the packets. For these reasons, no application, host, or network component *should* ever crash based on an Nmap scan. If they do, that is a bug in the system which should be repaired by the vendor.

Reports of systems being crashed by Nmap are rare, but they do happen. Many of these systems were probably unstable in the first place and Nmap either pushed them over the top or they crashed at the same time as an Nmap scan by pure coincidence. In other cases, poorly written applications, TCP/IP stacks, and even operating systems have been demonstrated to crash reproducibly given a certain Nmap command. These are usually older legacy devices, as newer equipment is rarely released with these problems. Smart companies use Nmap and many other common network tools to test devices prior to shipment. Those who omit such pre-release testing often find out about the problem in early beta tests when a box is first deployed on the Internet. It rarely takes long for a given IP to be scanned as part of Internet background noise. Keeping systems and devices up-to-date with the latest vendor patches and firmware should reduce the susceptibility of your machines to these problems, while also improving the security and usability of your network.

In many cases, finding that a machine crashes from a certain scan is valuable information. After all, attackers can do anything Nmap can do by using Nmap itself or their own custom scripts. Devices should not crash from being scanned and if they do, vendors should be pressured to provide a patch. In some usage scenarios, detecting fragile machines by crashing them is undesirable. In those cases you may want to perform very light scanning to reduce the risk of adverse effects. Here are a few suggestions:

- Use SYN scan (-sS) instead of connect scan (-sT). User-mode applications such as web servers can rarely even detect the former because it is all handled in kernel space and thus the services have no excuse to crash.
- Version scanning (-sV) and some of our NSE scripts (-sC or --script) risk crashing poorly written applications. Similarly, some buggy operating systems have been reported to crash when OS fingerprinted (-O). Omit these options for particularly sensitive environments or where you do not need the results.
- Using -T2 or slower (-T1, -T0) timing modes can reduce the chances that a port scan will harm a system, though they slow your scan dramatically. Older Linux boxes had an identd daemon that would block services temporarily if they were accessed too frequently. This could happen in a port scan, as well as during legitimate high-load situations. Slower timing might help here. These slow timing modes should only be used as a last resort because they can slow scans by an order of magnitude or more.
- Limit the number of ports and machines scanned to the fewest that are required. Every machine scanned has a minuscule chance of crashing, and so cutting the number of machines down improves your odds. Reducing the number of ports scanned reduces the risks to end hosts as well as network devices. Many NAT/firewall devices keep a state entry for every port probe. Most of them expire old entries when the table fills up, but occasional (pathetic) implementations crash instead. Reducing the ports and hosts scanned reduces the number of state entries and thus might help those fragile and defective devices stay up

Next tool we are going to use is Nikto.

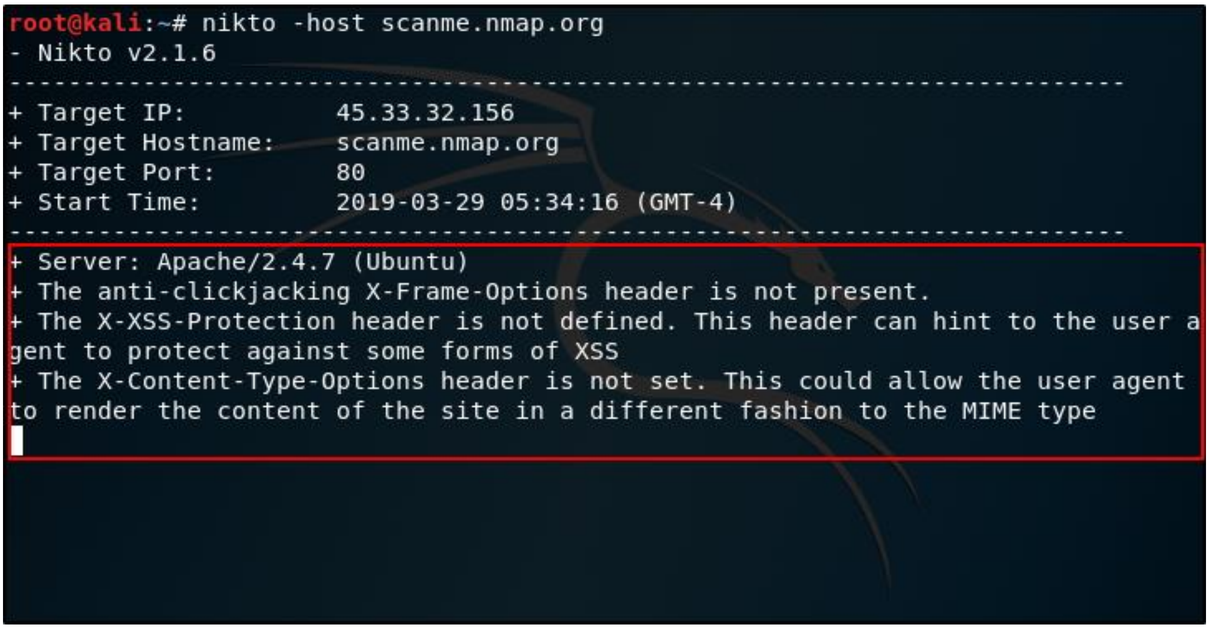
Nikto for Network Scanning

Nikto is a Web Server Scanner that tests for dangerous files and outdated service software. And these details can be exploited and used to hack the network. Nikto is designed to scan the web server in the quickest possible time.

To use Nikto, open the terminal and run the following command:

```
$ nikto -host scanme.nmap.org
```

You should see a similar output



```
root@kali:~# nikto -host scanme.nmap.org
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2019-03-29 05:34:16 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
```

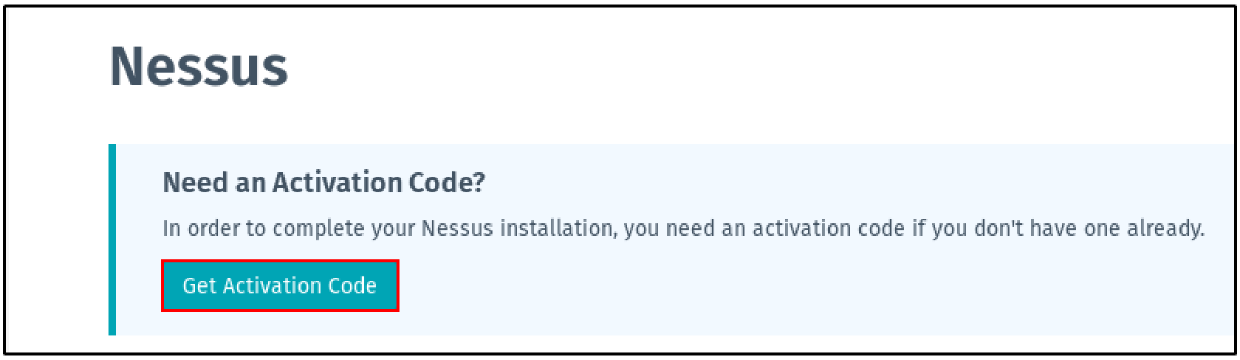
The highlighted part in the above screenshot shows the results that Nikto has found. These results are helpful to understand the weaknesses of the network or application being scanned. Once you find the weakness of the network, you can choose relevant attacks to hack the network.

The next tool I am going to talk about is Nessus.

Nessus for Network Scanning

Nessus is one of the most powerful vulnerability scanners available. This scanner does not come pre-installed with Kali Linux. So, before telling how to use it, I will show you how to install it.

Open a browser and go to www.tenable.com/downloads/nessus and click on "**Get Activation Code**".

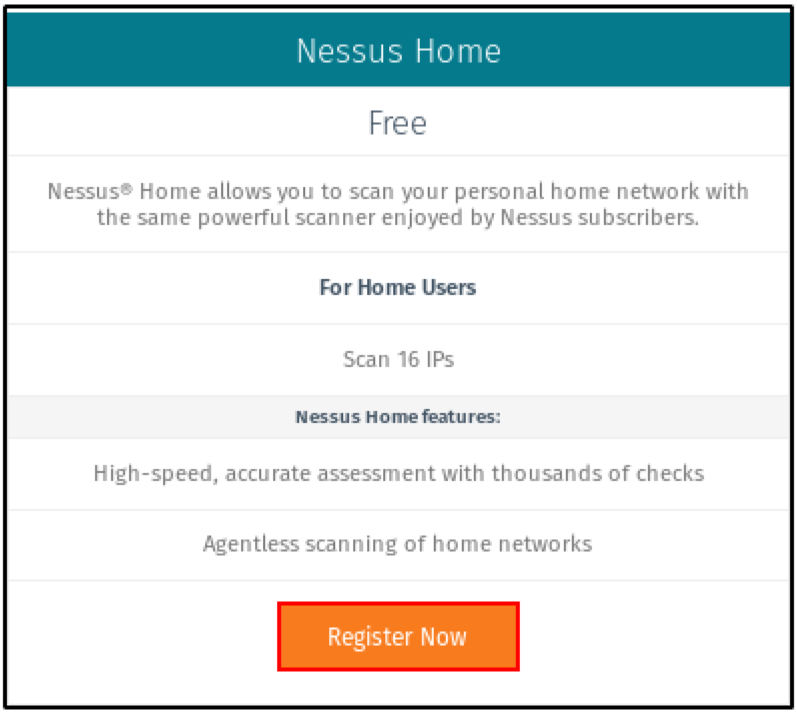


Nessus

Need an Activation Code?

In order to complete your Nessus installation, you need an activation code if you don't have one already.

You will see two versions of Nessus: A free version(Nessus Home) and a paid version. We shall use the free version, so click on the "**Register Now**" button under "**Nessus Home**".



Nessus Home

Free

Nessus® Home allows you to scan your personal home network with the same powerful scanner enjoyed by Nessus subscribers.

For Home Users

Scan 16 IPs

Nessus Home features:

High-speed, accurate assessment with thousands of checks

Agentless scanning of home networks

Now some of the most common enumeration techniques and discuss how they can be used in ethical hacking.

Enumeration in Ethical Hacking

Enumeration is extracting a system's valid usernames, machine names, share names, directory names, and other information. It is a key component of ethical hacking and penetration testing, as it can provide attackers with a wealth of information that can be used to exploit vulnerabilities. It can also be defined as collecting detailed information about the target systems, such as operating and network infrastructure details. Enumeration can be used in both an offensive and defensive manner.

Enumeration is one of the most important steps in ethical hacking because it gives hackers the necessary information to launch an attack. For example, hackers who want to crack passwords need to know the usernames of valid users on that system. Enumerating the target system can extract this information (CrashTestSecurity.com, 2022).

Enumeration can be used to gather any of the following information:

- Operating system details
- Network infrastructure details
- Usernames of valid users
- Machine names
- Share names
- Directory names
- Printer names
- Web server details

Why Is Enumeration Important?

Enumeration lets you understand what devices are on your network, where they are located, and what services they offer. To put it simply, enumeration can be used to find security vulnerabilities within systems and networks. By conducting an enumeration scan, you can see what ports are open on devices, which ones have access to specific services, and what type of information is being transmitted. This information can then be used to exploit weaknesses and gain unauthorized access.

Carrying out an enumeration scan requires both time and patience. However, it’s a crucial step in the hacking process as it allows you to gather intelligence about your target. Enumeration can be performed manually or with automated tools. Whichever method you choose, it’s important to be thorough in your scan to maximize the amount of information you can collect.

Techniques for Enumeration

When it comes to network security, enumeration is key. By enumerating a system, you can gain a better understanding of that system and how it works. This knowledge can then be used to exploit vulnerabilities and gain access to sensitive data.

Several techniques can be used for enumeration, and your method will depend on the type of system you are targeting. The most common methods include email IDs and usernames, default passwords, and DNS zone transfer.

- Using email IDs and usernames is a great way to gather information about a system. You can use this information to brute force passwords or gain access to sensitive data. Default passwords are another common method of enumeration.
- By using default passwords, you can gain access to systems that have not been properly configured.
- DNS zone transfer is a technique that can be used to expose topological information. This information can be used to identify potential targets for attack.

Understanding the techniques available for enumeration can better protect your systems from attack.

Process of Enumeration

Enumeration is the process of identifying all hosts on a network. This can be done in several ways, but active and passive scanning is the most common method. Active scanning involves sending out requests and analyzing the responses to determine which hosts are active on the network. Passive scanning involves listening to traffic and then analyzing it to identify hosts.

Both methods have their advantages and disadvantages. Active scanning is more likely to identify all hosts on a network, but it is also more likely to cause disruptions because it generates a lot of traffic. Passive scanning is less likely to identify all hosts, but it is also less likely to cause disruptions because it does not generate any traffic.

The Types of Enumeration

There are many different types of enumeration. The most appropriate type will depend on the situation and the required information:

- **NetBIOS Enumeration:** NetBIOS is a protocol that allows devices on a network to share resources and communicate with each other. NetBIOS enumeration is querying a device to identify what NetBIOS resources are available. This can be done using tools like **nbtstat** and **net view**.
- **SNMP Enumeration:** SNMP is a protocol that allows devices to be managed and monitored remotely. SNMP enumeration is querying a device to identify what SNMP resources are available. This can be done using tools like **SNMP-check** and **snmpwalk**.
- **LDAP Enumeration:** LDAP is a protocol that allows devices on a network to share information about users and resources. LDAP enumeration is querying a device to identify what LDAP resources are available. This can be done using tools like **ldapsearch** and **ldapenum**.

- **NTP Enumeration:** NTP is a protocol that allows devices on a network to synchronize their clocks with each other. NTP enumeration is querying a device to identify what NTP resources are available. This can be done using tools like **Nmap** and **PRTG Network Monitor** (CrashTestSecurity.com, 2022).

Services and Ports to Enumerate

When conducting a penetration test or simply enumerating services on a target machine, knowing which ports are associated with it is often useful. This can be accomplished using a port scanner such as Nmap to scan for open ports on the target machine. Once you have a list of open ports, you can use a port lookup tool to determine which service runs on each port. This information can be extremely helpful when trying to identify potential attack vectors.

The following are some of the most commonly used services and their associated ports:

- FTP – 21
- SSH – 22
- HTTP – 80
- HTTPS – 443
- SMTP – 25
- POP3 – 110
- IMAP – 143
- SNMP – 161

As you can see, various services can run on any given port. Knowing which service runs on which port when enumerating a target machine is helpful.

Enumeration, also known as information gathering, is the first phase of ethical hacking. To establish your career as an ethical hacker, you must know all the stages, tools, techniques, attack vectors, and surfaces to identify weak links.

4. How does Google Hacking contribute to footprinting and information gathering in ethical hacking?

A footprint is a digital trace of your activity that you leave behind on the Internet. It is like the footprint you leave behind in the sand at the beach. These footprints can be innocuous, such as an e-mail account that you have forgotten about in Hotmail, or they can give away highly sensitive information through your browsing history on your work computer.

Footprints also include information about what social networks and other websites people visit, what content they look at and for how long, who their Facebook friends are, and when they were last online; all this data is available with just one click to Google or to a range of specialized search engines.

Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.

The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners. This information includes the OS used by the organization, firewalls, network maps, IP addresses, domain name system information, security configurations of the target machine, URLs, virtual private networks, staff IDs, email addresses and phone numbers.

There are two types of footprinting in ethical hacking:

1. active footprinting
2. passive footprinting

What is active footprinting?

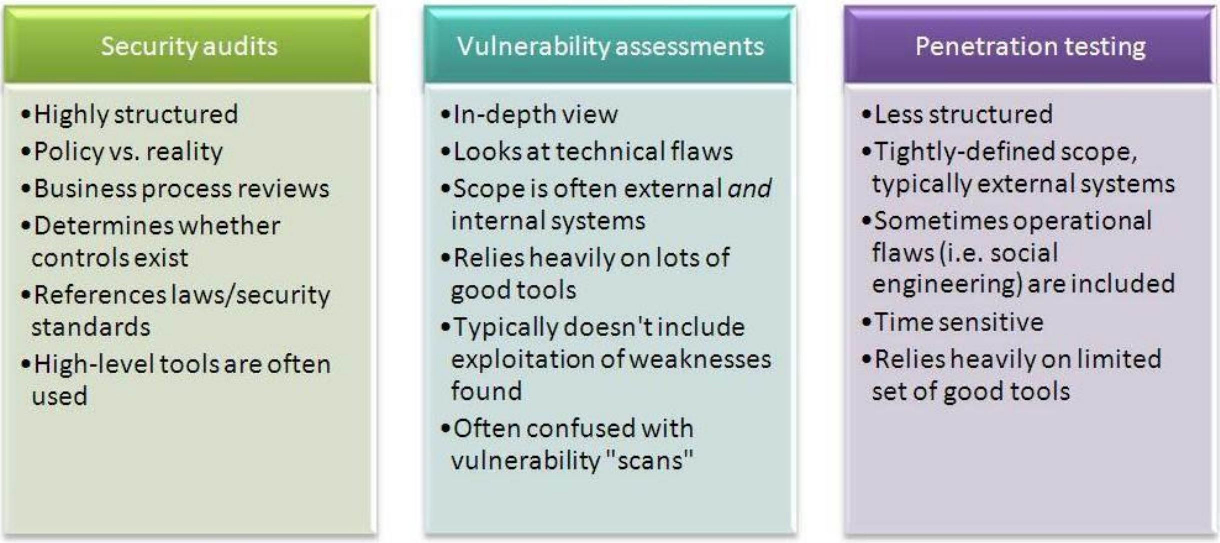
Active footprinting describes the process of using tools and techniques, like using the traceroute commands or a ping sweep -- Internet Control Message Protocol sweep -- to collect data about a specific target. This often triggers the target's intrusion detection system (IDS). It takes a certain level of stealth and creativity to evade detection successfully.

What is passive footprinting?

As the name implies, passive footprinting involves collecting data about a specific target using innocuous methods, like performing a Google search, looking through Archive.org, using NeoTrace, browsing through employees' social media profiles, looking at job sites and using Whois, a website that provides the domain names and associated networks fora specific organization. It is a stealthier approach to footprinting because it does not trigger the target's IDS.

How do you start footprinting?

Reconnaissance is similar to footprinting and is a crucial part of the initial hacking exercise. It is a passive footprinting exercise where one collects data about the target's potential vulnerabilities and flaws to exploit while penetration testing.



Security audits	Vulnerability assessments	Penetration testing
•Highly structured •Policy vs. reality •Business process reviews •Determines whether controls exist •References laws/security standards •High-level tools are often used	•In-depth view •Looks at technical flaws •Scope is often external *and* internal systems •Relies heavily on lots of good tools •Typically doesn't include exploitation of weaknesses found •Often confused with vulnerability "scans"	•Less structured •Tightly-defined scope, typically external systems •Sometimes operational flaws (i.e. social engineering) are included •Time sensitive •Relies heavily on limited set of good tools

Footprinting can help ethical hackers find potential vulnerabilities to assess and test.

Footprinting processes start with determining the location and objective of an intrusion. Once ethical hackers identify a specific target, they gather information about the organization using nonintrusive methods, such as accessing the organization's own webpage, personnel directory or employee bios.

Ethical hackers collect this information and initiate social engineering campaigns to identify security vulnerabilities and achieve ethical hacking goals.

Advantages of footprinting

Footprinting techniques in ethical hacking help businesses identify and secure IT infrastructure before a **threat actor** exploits a vulnerability. Users can also build a database of known vulnerabilities and loopholes.

Footprinting also helps companies better understand their current **security posture** through analysis of data gathered about the firewall, security configuration and more. Users can update this list periodically and use it as a reference point during security audits.

Drawing a network map helps cover all trusted **routers**, servers and other **network topologies.** Users can pursue a reduced attack surface by narrowing it down to a specific range of systems.

Other types of footprinting

DNA footprinting is the method used to identify the nucleic acid sequence that binds with proteins.

An **ecological footprint** is an approach to measuring human demand for natural capital or resources. It calculates the amount of natural resources required to support people or an economy. Ecological footprinting uses an ecological accounting system to keep track of this demand.

A **digital footprint** describes one's unique, traceable digital activities. These include actions, communications and contributions expressed on the internet or digital services. Digital footprints can be either active or passive.

Primary Sources:

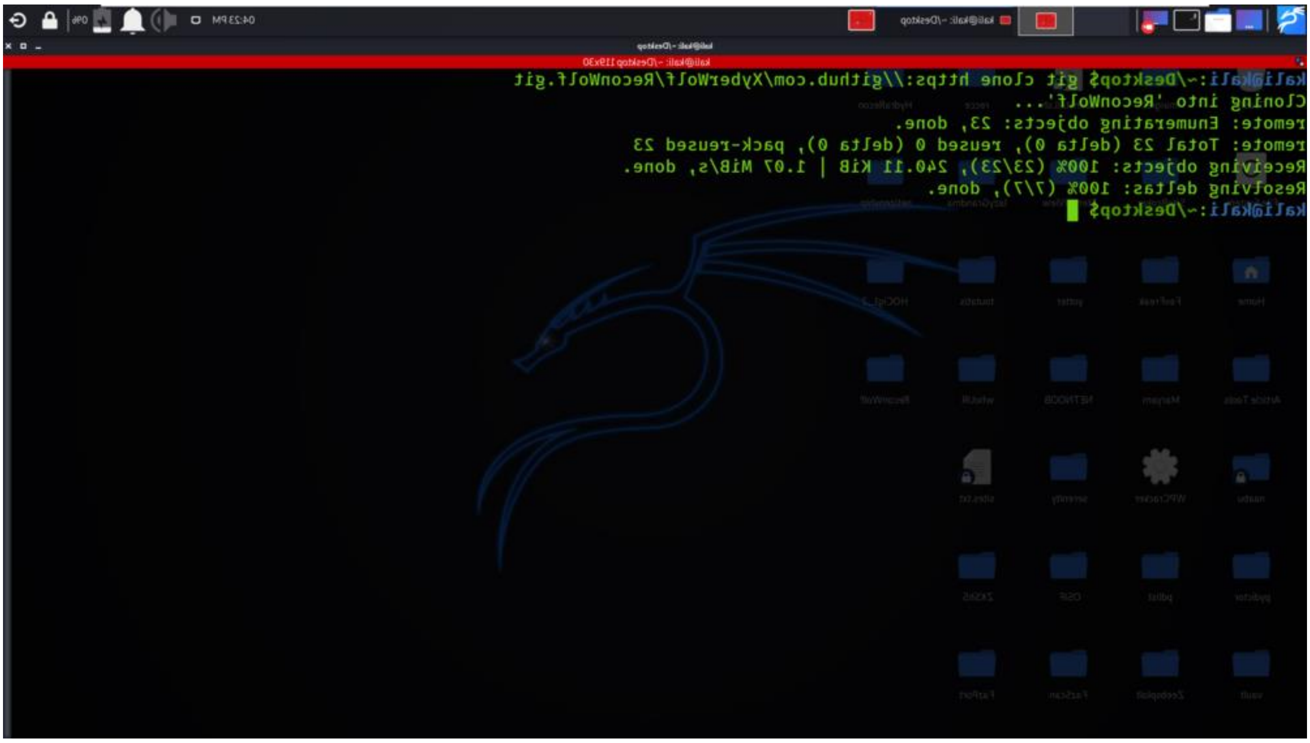
In general, websites and search engines like Google and Bing allow you to create a footprint about yourself by disclosing your name, address, phone numbers, and other information about yourself. This information is then stored and can be found by anyone. Information about you on the web may be used to identify additional information about your **social networks** or connections. There are a number of software tools that can help find out more information about a person, company, or organization that has been the subject of an investigation. These include:

- Footprinting is essential to identity theft hackers, who must gather as much detailed information on the identities and activities of their targets as possible in order to establish whether enough evidence exists for them to consider a fraud report to the police.
- The Internet allows for a revolution in the way people collect personal information.
- The tool which has been used is e-mail passwords, which are emails that have been sent by an email address.
- This makes it easy for criminals to steal the password for the e-mail and thus gain access to all of their online activities and a lot of their personal information.
- There are many people that do not use their passwords and do not change them often. There are also many people that choose not to use a password at all and still use the same password over and over again.

Installation of Reconwolf Tool on Kali Linux OS:

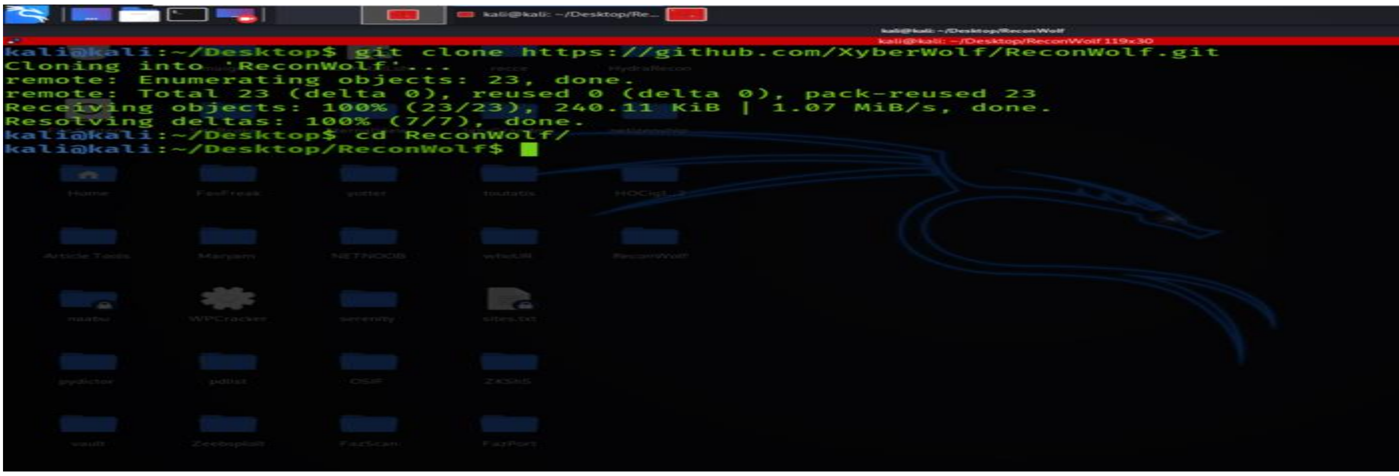
Step 1: Use the following command to install the tool in your Kali Linux operating system.

git clone https://github.com/XyberWolf/ReconWolf.git



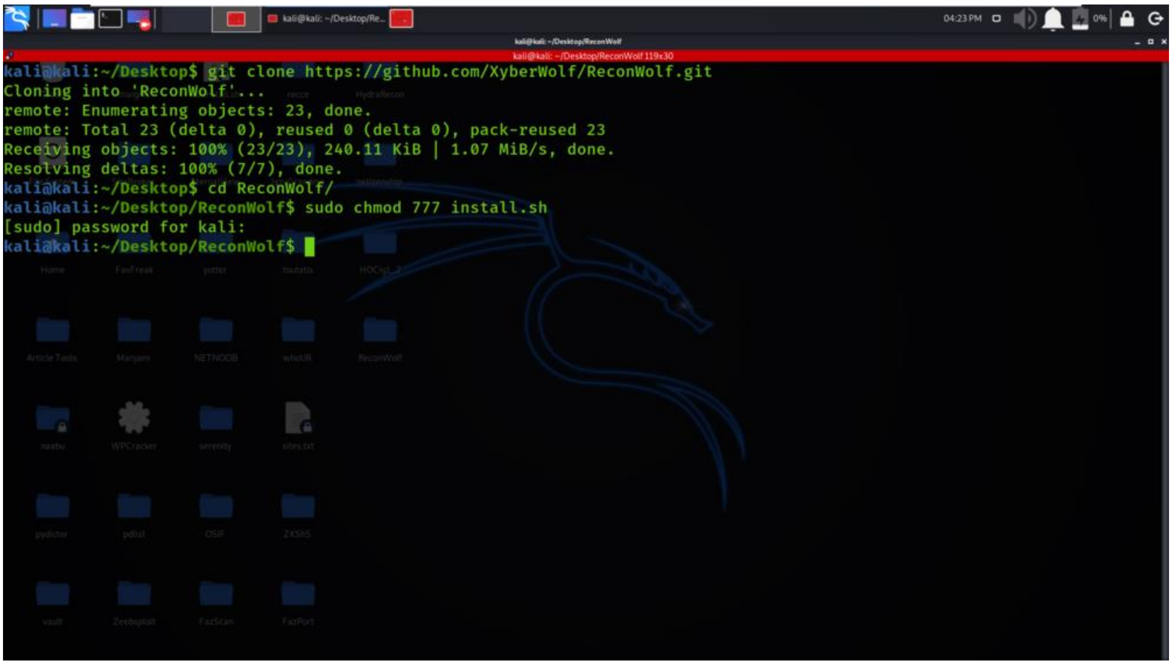
```
kali@kali:~/Desktop$ git clone https://github.com/XyberWolf/ReconWolf.git
Cloning into 'ReconWolf'...
remote: Enumerating objects: 23, done.
remote: Total 23 (delta 0), reused 0 (delta 0), pack-reused 23
Receiving objects: 100% (23/23), 240.11 KiB | 1.07 MiB/s, done.
Resolving deltas: 100% (7/7), done.
kali@kali:~/Desktop$
```

Step 2: Now use the following command to move into the directory of the tool. You have to move in the directory in order to run the tool.
cd ReconWolf



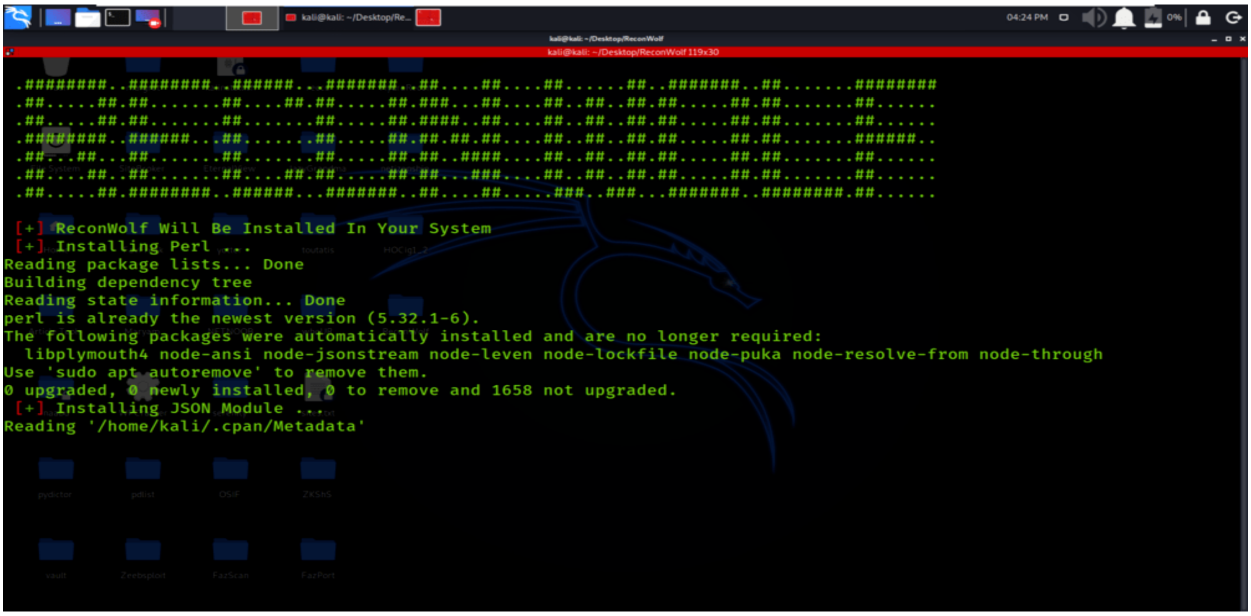
```
kali@kali:~/Desktop$ git clone https://github.com/XyberWolf/ReconWolf.git
Cloning into 'ReconWolf'...
remote: Enumerating objects: 23, done.
remote: Total 23 (delta 0), reused 0 (delta 0), pack-reused 23
Receiving objects: 100% (23/23), 240.11 KiB | 1.07 MiB/s, done.
Resolving deltas: 100% (7/7), done.
kali@kali:~/Desktop$ cd ReconWolf/
kali@kali:~/Desktop/ReconWolf$
```

Step 3: Change the permissions of the install.sh file by using the following command.
sudo chmod 777 install.sh



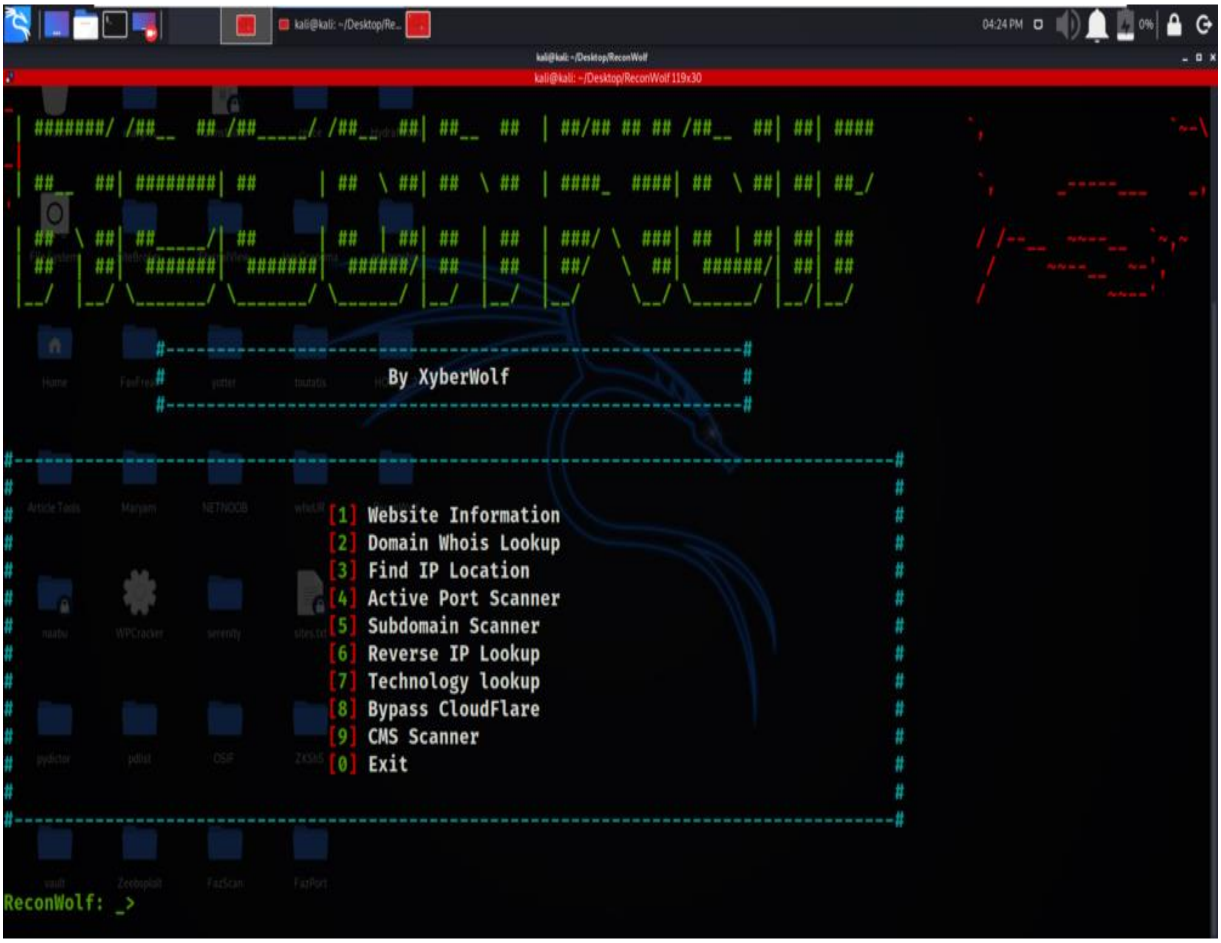
```
kali@kali:~/Desktop$ git clone https://github.com/XyberWolf/ReconWolf.git
Cloning into 'ReconWolf'...
remote: Enumerating objects: 23, done.
remote: Total 23 (delta 0), reused 0 (delta 0), pack-reused 23
Receiving objects: 100% (23/23), 240.11 KiB | 1.07 MiB/s, done.
Resolving deltas: 100% (7/7), done.
kali@kali:~/Desktop$ cd ReconWolf/
kali@kali:~/Desktop/ReconWolf$ sudo chmod 777 install.sh
[sudo] password for kali:
kali@kali:~/Desktop/ReconWolf$
```

Step 4: Run the below command to verify the installation.
./install.sh



```
.########..########..######...#######..##....##....##......##..#######..##.......########
.##.....##.##.......##....##.##.....##.###...##....##..##..##.##.....##.##.......##......
.##.....##.##.......##.......##.....##.####..##....##..##..##.##.....##.##.......##......
.########..######...##.......##.....##.##.##.##....##..##..##.##.....##.##.......######..
.##...##...##.......##.......##.....##.##..####....##..##..##.##.....##.##.......##......
.##....##..##.......##....##.##.....##.##...###....##..##..##.##.....##.##.......##......
.##.....##.########..######...#######..##....##.....###..###...#######..########.##......

 [+] ReconWolf Will Be Installed In Your System
 [+] Installing Perl ...
Reading package lists... Done
Building dependency tree
Reading state information... Done
perl is already the newest version (5.32.1-6).
The following packages were automatically installed and are no longer required:
  libplymouth4 node-ansi node-jsonstream node-leven node-lockfile node-puka node-resolve-from node-through
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1658 not upgraded.
 [+] Installing JSON Module ...
Reading '/home/kali/.cpan/Metadata'
```



```
| #######/ /##__  ## /##____/ /##__##| ##__  ##  | ##/## ## ## /##__  ##| ##| ####

| ##__  ##| ########| ##      | ##  \ ##| ##  \ ##  | ####_  ####| ##  \ ##| ##| ##_/

| ##  \ ##| ##_____/| ##      | ##  | ##| ##  | ##  | ###/ \  ###| ##  | ##| ##| ##
| ##  | ##|  #######|  #######|  ######/| ##  | ##  | ##/   \  ##|  ######/| ##| ##
|__/  |__/ \_______/ \_______/ \______/ |__/  |__/  |__/     \__/ \______/ |__/|__/

               #----------------------------------------------------------#
               #                       By XyberWolf                       #
               #----------------------------------------------------------#

#-------------------------------------------------------------------------------------------#
#                                                                                           #
#                                 [1] Website Information                                   #
#                                 [2] Domain Whois Lookup                                   #
#                                 [3] Find IP Location                                      #
#                                 [4] Active Port Scanner                                   #
#                                 [5] Subdomain Scanner                                     #
#                                 [6] Reverse IP Lookup                                     #
#                                 [7] Technology lookup                                     #
#                                 [8] Bypass CloudFlare                                     #
#                                 [9] CMS Scanner                                           #
#                                 [0] Exit                                                  #
#                                                                                           #
#-------------------------------------------------------------------------------------------#

ReconWolf: _>
```

Countermeasures:

In most cases, when someone is using their username and password, that is the same as their email address or an e-mail from another provider, then this just adds to the list of information that is on the thief's computer. What you want to do is make sure that the username and password aren't something that can be found online by anyone.

- **Using an IP address:** An IP (Internet Protocol) address is a number given to devices connected to the Internet. It lets devices know where they are geographically so that they can send data back and forth across networks and computers properly. Sometimes, though, these numbers can be used as tracking measures as well, which could reveal a person's location through their computer. Some computers make it simple to obtain their IP address by using their computer's built-in Internet connection, but this can also be achieved by using a proxy server. Proxy servers are often used for anonymizing internet traffic.
- **Using search queries:** If your IP address is only one of many being searched, then in most cases the search results will note an IP address first and won't even bother to look for other information. Anonymizers are sometimes used so that no information is given away at all if possible. **Using geolocation**: In the United States, software such as Google and Foursquare are available to help locate a person's location using their IP address. In some cases, this can be traced back to the individual who was using their computer at that time.
- **Where possible, using alternative services:** Most commonly people will use their e-mail or browser settings to try and mask their actual IP address. If they have used a proxy server though or are accessing other encrypted websites then there is no way of finding out that they have done so. This is one reason why anonymizers should not be used since it reveals exactly where you are located geographically.

Conclusion:

There are many ways that your digital footprint can be collected and used against you. This can be done by a third party or even by yourself. In most cases using search engines like Google, Bing and Yahoo! will be the easiest way to find out information about you or anyone else that has an e-mail address.

A great deal of effort is put into trying to cover up all the information on the internet about you, but once it is out there it can never really be taken back. It may not become public knowledge immediately, but if someone wants to learn something then they will most likely find what they are looking for eventually.

5. Describe the significance of networking fundamentals in the context of ethical hacking and incident response planning (IRP)

Ethical hacking is a process of detecting vulnerabilities in an application, system or organization's infrastructure that an attacker can use to exploit an individual or organization they use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points. In the world of ethical hacking, understanding network basics and popular protocols is essential. A hacker's success often depends on their ability to navigate and exploit network vulnerabilities various network attacks, and strategies to protect against them in cyber security.

What is Network Hacking

Network hacking refers to the act of gaining unauthorized access to a computer network and its infrastructure resources, such as devices, servers, software, and other services.

Network hacking involves gathering information about a target network, identifying vulnerabilities, and exploiting them to gain access. A variety of tools and techniques are used to identify potential security threats in computer networks.

Network Fundamentals

Understanding the concept of network hacking effectively requires a solid understanding of the fundamentals of networking. These include understanding what networks are, types of networks such as LAN and WAN, communication protocols such as TCP/IP and HTTP, the concept of ports and services, and the role of devices such as routers, switches, and servers in facilitating network connectivity and data transmission.

Steps Involved in Network Hacking

The steps involved in network hacking within an ethical hacking context typically include:

1. Reconnaissance

This phase involves gathering information about the target network, such as IP addresses, domain names, network infrastructure, and other publicly available information. It may include techniques like open-source intelligence (OSINT) gathering, scanning public databases, or using tools like WHOIS to obtain domain registration information.

2. Scanning

In this phase, the ethical hacker uses network scanning tools to discover active systems, open ports, and services running on the target network. Techniques like port scanning, network mapping, and vulnerability scanning are employed to identify potential entry points or weaknesses.

3. Enumeration

Once active systems and services are identified, the ethical hacker attempts to gather more detailed information about those systems, such as user accounts, network shares, or system configurations. This helps in identifying potential vulnerabilities or misconfigurations that could be exploited.

4. Exploitation

In this stage, the ethical hacker attempts to exploit identified vulnerabilities to gain unauthorized access or escalate privileges. Exploitation techniques may include using known exploits, social engineering, or password cracking. The objective is to validate the existence and severity of vulnerabilities.

5. Post-Exploitation

After successfully exploiting a vulnerability, ethical hackers explore the compromised system to understand the extent of the potential damage that a malicious attacker could inflict. This helps assess the risks and consequences of a breach.

Types of Network Attacks

Network attacks can target different layers of the network stack, from physical infrastructure to application layer protocols. Some common types of network attacks include:

1. Denial-of-Service (DoS) Attack

A DoS attack overwhelms networks, systems or services with excessive traffic or requests, making them unavailable to legitimate users.

2. Man-in-the-Middle (MitM) Attack

In a MitM attack, attackers intercept and eavesdrop on network communications between two parties, allowing them to capture sensitive information or manipulate the data being transmitted.

3. IP Spoofing Attack

IP spoofing is a technique where an attacker falsifies the source IP address in an IP packet to make it appear as if it originated from a different source than the actual sender.

4. ARP Spoofing Attack

ARP spoofing, also known as ARP cache poisoning, is an attack where an attacker manipulates the Address Resolution Protocol (ARP) to intercept or manipulate network traffic.

5. Privilege Escalation Attack

Privilege escalation attacks involve exploiting vulnerabilities or weaknesses in a system to gain higher levels of access or permissions than originally granted, typically allowing attackers to execute unauthorized actions or access sensitive resources.

How to Prevent Network Hacking?

Preventing network attacks is crucial for maintaining the security and integrity of computer networks.

Here are some key measures and best practices to help prevent cyber attacks:

1. Deploy a Robust Firewall
2. Deploy Intrusion Detection and Prevention Systems (IDS/IPS)
3. Implement Strong Data Encryption
4. Implement Strong Access Controls
5. Conduct Regular Vulnerability Assessments and Penetration Testing

6. Implement Comprehensive Network Monitoring
7. Regular Updates and Patching

Network hacking is a complex and multifaceted field within cybersecurity. Understanding its fundamentals, types of attacks, the steps involved, and prevention strategies is crucial for individuals and organizations to protect their networks and sensitive data.

While malicious hacking poses significant threats to individuals and organizations, ethical hacking plays a vital role in identifying and mitigating vulnerabilities within computer networks.

What is incident response?

Incident response (sometimes called cybersecurity incident response) refers to an organization's processes and technologies for detecting and responding to cyberthreats, security breaches or cyberattacks. A formal incident response plan enables cybersecurity teams to limit or prevent damage.

The goal of incident response is to prevent cyberattacks before they happen, and to minimize the cost and business disruption resulting from any cyberattacks that occur.

Ideally, an organization defines incident response processes and technologies in a formal incident response plan (IRP) that specifies exactly how different types of cyberattacks should be identified, contained, and resolved. An effective incident response plan can help cybersecurity teams detect and contain cyberthreats and restore affected systems faster, and reduce the lost revenue, regulatory fines, and other costs associate with these threats. IBM's Cost of a Data Breach 2022 Report found that organizations with incident response teams and regularly tested incident response plans had an average data breach cost USD 2.66 million lower than that of organizations without incident response teams and IRPs.

Gain insights to prepare and respond to cyberattacks with greater speed and effectiveness with the IBM Security X-Force Threat Intelligence Index.

What are security incidents?

A security incident, or security event, is any digital or physical breach that threatens the confidentiality, integrity, or availability or an organization’s information systems or sensitive data. Security incidents can range from intentional cyberattacks by hackers or unauthorized users, to unintentional violations of security policy by legitimate authorized users.

Some of the most common security incidents include:

1. Ransomware
2. Phishing and social engineering
3. DDoS attacks
4. Supply chain atttacks
5. Insider threats

Ransomware: Ransomware is a type of malicious software, or malware, that locks up a victim's data or computing device and threatens to keep it locked—or worse—unless the victim pays the attacker a ransom. According to IBM's *Cost of a Data Breach 2022* report, ransomware attacks rose by 41 percent between 2021 and 2022.

Phishing and social engineering: Phishing attacks are digital or voice messages that try to manipulate recipients into sharing sensitive information, download malicious software, transferring money or assets to the wrong people, or take some other damaging action. Scammers craft phishing messages to look or sound like they come from a trusted or credible organization or individual—sometimes even an individual the recipient knows personally.

Phishing is the most costly and second most common cause of data breaches, according to IBM's Cost of a Data Breach 2022 report. It’s also the most common form of social engineering—a class of attack that hacks human nature, rather than digital security vulnerabilities, to gain unauthorized access to sensitive personal or enterprise data or assets.

DDoS attacks: In a distributed denial-of-service (DDoS) attack, hackers gain remote control of large numbers of computers and use them to overwhelm a target organization’s network or servers with traffic, making those resources unavailable to legitimate users.

Supply chain attacks: Supply chain attacks are cyberattacks that infiltrate a target organization by attacking its vendors—for example, by stealing sensitive data from a supplier’s systems, or by using a vendor’s services to distribute malware. In July 2021, cybercriminals took advantage of a flaw in Kaseya's VSA platform (link resides outside ibm.com) to spread ransomware to customers under the guise of a legitimate software update. Even though supply chain attacks are increasing in frequency, only 32 percent of organizations have incident response plans prepared for this particular cyberthreat, according to IBM's 2021 Cyber Resilient Organization Study.

Insider threats: There are two types of insider threats. *Malicious* insiders are employees, partners, or other authorized users who intentionally compromise an organization's information security. Negligent insiders are authorized user who unintentionally compromise security by failing to follow security best practices—by, say, using weak passwords, or storing sensitive data in insecure places.

Incident response planning

As noted previously, an organization's incident response efforts are guided by an incident response plan. Typically these are created and executed by a computer security incident response team (CSIRT) made up of stakeholders from across the organization—the chief information security officer (CISO), security operations center (SOC) and IT staff, but also representatives from executive leadership, legal, human resources, regulatory compliance, and risk management.

An incident response plan usually includes

- The roles and responsibilities of each member of the CSIRT;
- The security solutions—software, hardware, and other technologies—to be installed across the enterprise.
- A business continuity plan outlining procedures for restoring critical affected systems and data as quickly as possible in the event of an outage;
- A detailed incident response methodology that lays out the specific steps to be taken at each phase of the incident response process, and by whom;
- A communications plan for informing company leaders, employees, customers, and even law enforcement about incidents;
- Instructions for documenting for collecting information and documenting incidents for post-mortem review and (if necessary) legal proceedings.

It's not uncommon for the CSIRT to draft different incident response plans for different types of incidents, as each type may require a unique response. According to the IBM® 2021 Cyber Resilient Organization

Study, most organizations have specific incident response plans pertaining to DDoS attacks, malware and ransomware, and phishing, and nearly half have plans for insider threats.

Some organizations supplement in-house CSIRTs with external partners providing incident response services. These partners often work on retainer, assist with various aspects of the incident management process, including preparing and executing IRPs.

The incident response process

Most IRPs also follow the same general incident response framework based on incident response models developed by the SANS Institute, the National Institute of Standards and Technology (NIST), and the Cybersecurity and Infrastructure Agency (CISA).

Preparation: This first phase of incident response is also a continuous one, to make sure that the CSIRT always has the best possible procedures and tools in place to respond to identify, contain, and recover from an incident as quickly as possible and within minimal business disruption.

Through regular risk assessment the CSIRT identifies network vulnerabilities, defines the various types of security incidents that pose a risk to the network, and prioritizes each type according to its potential impact on the organization. Based on this risk assessment, the CSIRT may update existing incident response plans or draft new ones.

Detection and Analysis: During this phase, security team members monitor the network for suspicious activity and potential threats. They analyze data, notifications, and alerts gathered from device logs and from various security tools (antivirus software, firewalls) installed on the network, filtering out the false positives and triaging the actual alerts in order of severity.

Today, most organizations use one or more security solutions—such as SIEM (security information and event management) and EDR (endpoint detection and response)—to help security teams monitor and analyze security events in real time, and automate incident detection and response processes. (See “Incident response technologies” for more.)

The communication plan also comes into play during this phase. Once the CSIRT has determined what kind of threat or breach they're dealing with, they'll notify the appropriate personnel before moving to the next stage of the incident response process.

Containment: The incident response team takes steps to stop the breach from doing further damage to the network. Containment activities can be split into two categories:

- Short-term containment measures focus on preventing the current threat from spreading by isolating the affected systems, such as by taking infected devices offline.
- Long-term containment measures focus on protecting unaffected systems by placing stronger security controls around them, such as segmenting sensitive databases from the rest of the network.

At this stage, the CSIRT may also create backups of affected and unaffected systems to prevent additional data loss, and to capture forensic evidence of the incident for future study.

Eradication: After the threat has been contained, the team moves on to full remediation and complete removal of the threat from the system. This involves actively eradicating the threat itself—for example, destroying malware, booting an unauthorized or rogue user from the network—and reviewing both affected and unaffected systems to ensure that no traces of the breach are left behind.

Recovery: When the incident response team is confident the threat has been entirely eradicated, they restore affected systems to normal operations. This may involve deploying patches, rebuilding systems from backups, and bringing remediated systems and devices back online.

Post-incident review: Throughout each phase of the incident response process, the CSIRT collects evidence of the breach and documents the steps it takes to contain and eradicate the threat. At this stage, the CSIRT reviews this information to better understand the incident. The CSIRT seeks to determine the root cause of the attack, identify how it successfully breached the network, and resolve vulnerabilities so that future incidents of this type don't occur.

The CSIRT also reviews what went well and looks for opportunities to improve systems, tools, and processes to strengthen incident response initiatives against future attacks. Depending on the circumstances of the breach, law enforcement may also be involved in the post-incident investigation.

Incident response technologies

As noted above, in addition to describing the steps CSIRTs should take in the event of a security incident, incident response plans typically outline the security solutions that incident response teams should have in place to carry out or automate key incident response workflows, such as gathering and correlating security data, detecting incidents in real-time, and responding to in-progress attacks.

Some of the most commonly used incident response technologies include:

- **SIEM (security information and event management):** SIEM aggregates and correlates security event data from disparate internal security tools (for example firewalls, vulnerability scanners, threat intelligence feeds) and from devices on the network. SIEM can help incident response teams fight ‘alert fatigue’ by indicators of actual threats from the huge volume of notifications these tools generate.

- **SOAR (security orchestration, automation, and response):** SOAR enables security teams to define playbooks—formalized workflows that coordinate different security operations and tools in response to security incidents—and to automate portions of these workflows where possible.

- **EDR (endpoint detection and response):** EDR is software that is designed to automatically protect an organization's end users, endpoint devices and IT assets against cyberthreats that get past antivirus software and other traditional endpoint security tools. EDR collects data continuously from all endpoints on the network; it analyzes the data in real time for evidence of known or suspected cyberthreats, and can respond automatically to prevent or minimize damage from threats it identifies.

- **XDR (extended detection and response):** XDR is a cybersecurity technology that unifies security tools, control points, data and telemetry sources, and analytics across the hybrid IT environment (endpoints, networks, private and public clouds) to create a single, central enterprise system for threat prevention, detection, and response. A still-emerging technology, XDR has the potential to help overextended security teams and security operations centers (SOCs) do more with less by eliminating silos between security tools and automating response across the entire cyberthreat kill chain.

- **UEBA (user and entity behaviour analytics):** (UEBA) uses behavioural analytics, machine learning algorithms, and automation to identify abnormal and potentially dangerous user and device behaviour. UEBA is effective at identifying insider threats—malicious insiders or hackers that use compromised insider credentials—that can elude other security tools because they mimic authorized network traffic. UEBA functionality is often included in SIEM, EDR, and XDR solutions.

- **ASM (attach surface management):** ASM solutions automate the continuous discovery, analysis, remediation, and monitoring of the vulnerabilities and potential attack vectors across all the assets in an organization's attack surface. ASM can uncover previously unmonitored network assets, map relationships between assets.