Global Information Assurance Certification Paper

The Information We Seek

GIAC (GCIH) Gold Certification

Author: Jose Ramos, joseramostrd@gmail.com
Advisor: Adam Kliarsky
Accepted: October 16, 2016

Abstract

Whether you are performing a penetration test, conducting an investigation, or are skilled attackers closing in on a target, information gathering is the foundation that is needed to carry out the assessment. Having the right information paves the way for proper enumeration and simplifies attack strategies against a given target. Throughout this paper, we will walk through some strategies used to identify information on both people and networks. Some people claim that all data can be found using Google's search engine; but can third party tools found in Linux security distributions such as Kali Linux outperform the search engine giant? Maltego and The Harvester yield a wealth of information, but will the results be enough to identify a target? The right tool for the right job is essential when working with any project in life. Let's take a journey through the information gathering process to determine if there is a one size fits all tool, or if a multi-tool approach is needed to gather the essential information on a given target. We will compare and contrast many of the industry tools to determine the proper tool or tools needed to perform an adequate information gathering assessment.

Jose Ramos, joseramostrd@gmail.com

1. Introduction

It is the moment of truth. You are a penetration tester and tasked with finding and exploiting vulnerabilities for a new high profile client. This particular client has specifically requested for you to approach the testing like you were an attacker. Therefore, you were not provided with an IP range or contact details. Your palms begin to clam up as thoughts of losing your job start to circulate in your head due to the complexity of this task. Then you take a moment and think if an attacker performs this very function without detailed contacts and ranges, why can't a penetration tester do the same? The simple answer is that they can. With knowledge of what to look for and where to locate the information, this task can easily be achieved. Throughout this paper, we will go through many different methods of enumerating and identifying information. We will go through the many ways that information can be obtained (in transit and also at rest). It is common for people to attempt to safeguard their personal information, but the same individuals do not realize that the trusted organizations that they provide their information to might be at risk. We will use a trusted executive for a fortune 50 company as an example. The executive may know that attackers have been trying to spear fish him and the attackers will stop at nothing until they retrieve the information that his organization has entrusted him with. As a precaution, the executive use multi-factor authentication to access his email, he does not use public networks and is very adamant about discussing company secrets over a secure land line. The executive may believe that his and his company's information is secure. Assuming his information is secure may be his biggest problem. An attacker seeking information will not use conventional methods of infiltration when they are attempting to close in on their target. In fact, the attacker may wait till their target feels secure before they perform the attack. It is very rare that a burglar would walk through the front door of a home in broad daylight. The same concept applies to a hacker brute forcing the executive's email while making it obvious that the attack is occurring. Instead, an attacker may think outside the box. A stealthier approach would be to gain information on the target's family via social media and attempt to hack the weakest line of defense, for example the children. If an attacker can convince one of the children to open a crafted email containing a malicious payload on their home machine, this may be the way to gain access to the target information. A Meterpreter shell can be used to as a pivot point to enumerate the executive's home network further. Furthermore, the shell can also act as a key logger or be used to dump passwords out of memory.

Jose Ramos, joseramostrd@gmail.com

If an attacker wants to get the information, they will think of out of the box methods to achieve it. So let embark on a journey through the world of information and discuss various ways to obtain the data. This paper will discuss tools, techniques, and manual methods strategies used by both penetration testers and attackers. There are two goals of this paper; offensively identifying the right tools for the situation, and defensively how to protect against these types of attacks.

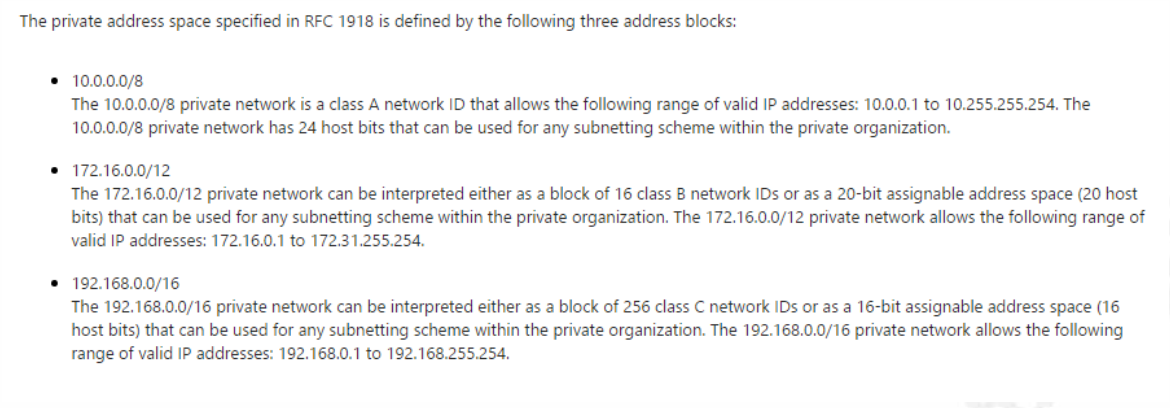
2. The Network

The first step during an information gathering assessment is to understand the information that you are attempting to obtain. For example, if a person was looking to get an IP range for a targeted network, they must first grasp the concept of how networks operate. Going in blindly would be similar to driving a car without the knowledge of traffic signs or street lights. Incorporating IP addresses that are not in a targets range can provide inconclusive results, or even worse, an assessment against a network that you were not authorized to perform. Let's drill down into this concept as it plays an important factor when it comes to gathering information about a targeted network. Networks are broken down into three different classes (A, B, and C). In addition to this breakdown, each of the classes has a reserved group of IP addresses that are meant for private use. The Microsoft TechNet website (Microsoft, n.d.) provides useful charts that can be utilized as a quick reference when deciphering between the different IP classes. Figure one identifies the various IP classes, and figure two shows the ranges that are reserved for private use.

Address Class	First Network ID	Last Network ID
Class A	1.0.0.0	126.0.0.0
Class B	128.0.0.0	191.255.0.0
Class C	192.0.0.0	223.255.255.0

Figure 1: IP Class range (Address classes, n.d.)

Jose Ramos, joseramostrd@gmail.com



The private address space specified in RFC 1918 is defined by the following three address blocks:

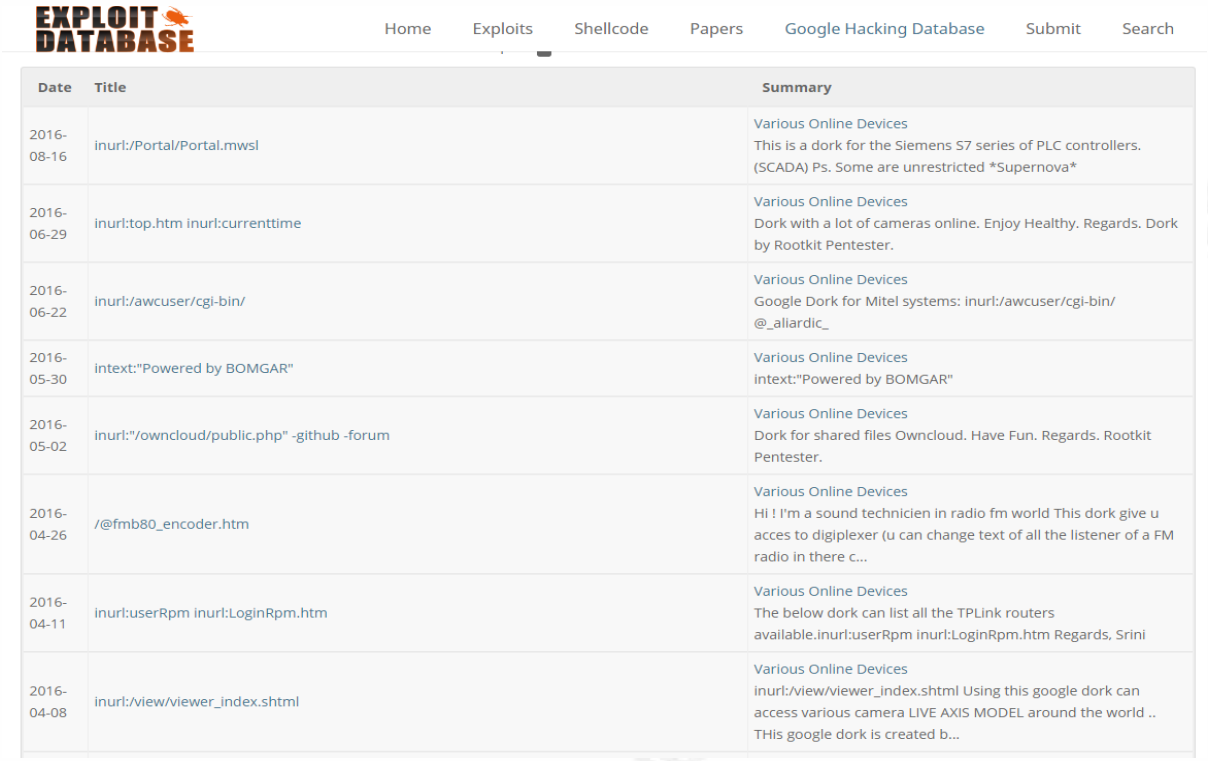
- 10.0.0.0/8
  The 10.0.0.0/8 private network is a class A network ID that allows the following range of valid IP addresses: 10.0.0.1 to 10.255.255.254. The 10.0.0.0/8 private network has 24 host bits that can be used for any subnetting scheme within the private organization.
- 172.16.0.0/12
  The 172.16.0.0/12 private network can be interpreted either as a block of 16 class B network IDs or as a 20-bit assignable address space (20 host bits) that can be used for any subnetting scheme within the private organization. The 172.16.0.0/12 private network allows the following range of valid IP addresses: 172.16.0.1 to 172.31.255.254.
- 192.168.0.0/16
  The 192.168.0.0/16 private network can be interpreted either as a block of 256 class C network IDs or as a 16-bit assignable address space (16 host bits) that can be used for any subnetting scheme within the private organization. The 192.168.0.0/16 private network allows the following range of valid IP addresses: 192.168.0.1 to 192.168.255.254.

Figure 2: Private address space (Public and private addresses, n.d.)

2.1 Search Engine Manipulation

Understanding a network is an important part of information gathering. However, the network does not always need to be scanned to enumerate information. Many of the times information is publically accessible; you simply need to search for the information differently. The Google web browser is a very powerful tool. Some ways have been discovered to manipulate this tool and find targeted information. In fact, the Exploit Database houses some these hacks that can be used to search for detailed information (Google hacking database, 2009). The image in Figure 3 illustrates a portion of the information found in the Network and Vulnerability section of the website. The “Inurl” text may not appear to be dangerous since it will generate random results. However, if you were to pair the exploitable system “Inurl" with the companies or a person's name, the results can present an immediate threat.

Jose Ramos, joseramostrd@gmail.com



EXPLOIT DATABASE

Home | Exploits | Shellcode | Papers | Google Hacking Database | Submit | Search

Date	Title	Summary
2016-08-16	inurl:/Portal/Portal.mwsl	Various Online Devices This is a dork for the Siemens S7 series of PLC controllers. (SCADA) Ps. Some are unrestricted *Supernova*
2016-06-29	inurl:top.htm inurl:currenttime	Various Online Devices Dork with a lot of cameras online. Enjoy Healthy. Regards. Dork by Rootkit Pentester.
2016-06-22	inurl:/awcuser/cgi-bin/	Various Online Devices Google Dork for Mitel systems: inurl:/awcuser/cgi-bin/ @_aliardic_
2016-05-30	intext:"Powered by BOMGAR"	Various Online Devices intext:"Powered by BOMGAR"
2016-05-02	inurl:"/owncloud/public.php" -github -forum	Various Online Devices Dork for shared files Owncloud. Have Fun. Regards. Rootkit Pentester.
2016-04-26	/@fmb80_encoder.htm	Various Online Devices Hi ! I'm a sound technicien in radio fm world This dork give u acces to digiplexer (u can change text of all the listener of a FM radio in there c...
2016-04-11	inurl:userRpm inurl:LoginRpm.htm	Various Online Devices The below dork can list all the TPLink routers available.inurl:userRpm inurl:LoginRpm.htm Regards, Srini
2016-04-08	inurl:/view/viewer_index.shtml	Various Online Devices inurl:/view/viewer_index.shtml Using this google dork can access various camera LIVE AXIS MODEL around the world .. THis google dork is created b...

Figure 3: Exploit database

Some other methods can be used to gather information about a particular target. The Exploit Database image shows a number strings that are tailored for specific devices; however, there are some other options used to find information on the target. An attacker can search for items in the body of a site, by a particular person or even a specified file type. The options are limitless, as an attacker can narrow down the specified information by combining two or more of these search criteria's into a single search. The SANS Institute has done a fantastic job of putting some of the key search items into a single which can be found at *www.sans.org/security-resources/GoogleCheatSheet.pdf*. The image in Figure 4 shows some the items that can be used to manipulate the search results when using the Google search engine.

Jose Ramos, joseramostrd@gmail.com

Advanced Operators		
Advanced Operators	**Meaning**	**What To Type Into Search Box *(& Description of Results)***
site:	Search only one website	**conference site:www.sans.org** *(Search SANS site for conference info)*
[#]...[#] or numrange:	Search within a range of numbers	**plasma television $1000...1500** *(Search for plasma televisions between $1000 and $1500)*
date:	Search only a range of months	**hockey date: 3** *(Search for hockey references within past 3 months; 6 and 12-month date-restrict options also available)*
safesearch:	Exclude adult-content	**safesearch: sex education** *(Search for sex education material without returning adult sites)*
link:	linked pages	**link:www.sans.org** *(Find pages that link to the SANS website)*
info:	Info about a page	**info:www.sans.org** *(Find information about the SANS website)*
related:	Related pages	**related:www.stanford.edu** *(Find websites related to the Stanford website)*
intitle:	Searches for strings in the title of the page	**intitle:conference** *(Find pages with "conference" in the page title)*
allintitle:	Searches for all strings within the page title	**allintitle:conference SANS** *(Find pages with "conference" and "SANS" in the page title. Doesn't combine well with other operators)*
inurl:	Searches for strings in the URL	**inurl:conference** *(Find pages with the string "conference" in the URL)*
allinurl:	Searches for all strings within the URL	**allinurl:conference SANS** *(Find pages with "conference" and "SANS" in the URL. Doesn't combine well with other operators)*
filetype: or **ext:**	Searches for files with that file extension	**filetype:ppt** *(Find files with the "ppt" file extension. ".ppt" are MS PowerPoint files.)*
cache:	Display the Google cache of the page	**cache:www.sans.org** *(Show the cached version of the page without performing the search)*
phonebook: or **rphonebook:** or **bphonebook**	Display all, residential, business phone listings	**phonebook:Rick Smith MD** *(Find all phone book listing for Rick Smith in Maryland. Cannot combine with other searches)*
author:	Searches for the author of a newsgroup post	**author:Rick** *(Find all newsgroup postings with "Rick" in the author name or email address. Must be used with a Google Group search)*
insubject:	Search only in the subject of a newsgroup post	**insubject:Mac OS X** *(Find all newsgroup postings with "Mac OS X" in the subject of the post. Must be used with a Google Group search)*
define:	Various definitions of the word or phrase	**define:sarcastic** *(Get the definition of the word sarcastic)*
stock:	Get information on a stock abbreviation	**stock:AAPL** *(Get the stock information for Apple Computer, Inc.)*

Figure 4: Google hacks

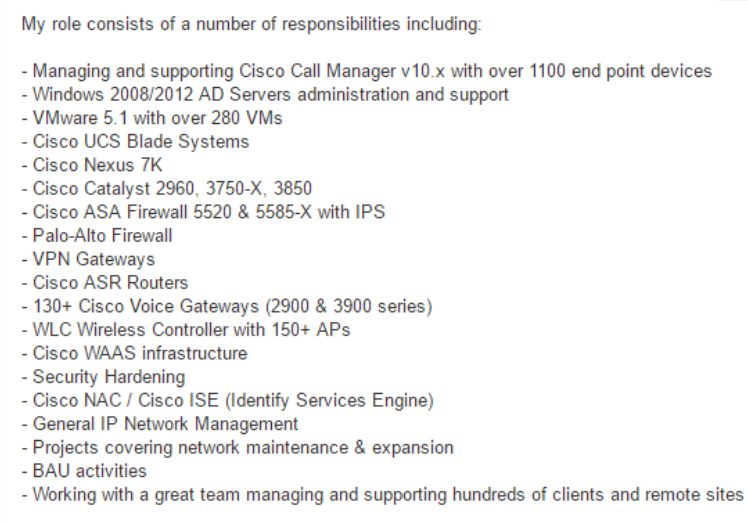
2.2 Discovered Information

Google is a very powerful tool for gathering information. A simple search result on a person's name often provides results about the individual. Social media information such as Facebook and LinkedIn are often top search results for name searches. Some would assume that an attacker would only use such information for identity theft of an individual; however, they are highly mistaken. Facebook accounts can be utilized as generate a password file on a target with tools that we will later discuss. It is common for people to use their animals or family names in passwords. Birthdays, anniversaries and maiden names are often mentioned in people's social media posts. The average person often chooses a name or number that they already remember when creating a password for an account. If all the names and numbers are posted within their social media account, an attacker can just pull the context of the posts and replay the

Jose Ramos, joseramostrd@gmail.com

information against a login. Another problem is that people are known to use the same password across many accounts. Therefore, there is a high chance that the same password used to breach a personal account can be used to compromise their corporate account as well.

LinkedIn is another great avenue for information gathering, especially when it comes to enumerating a network. LinkedIn is used primarily used to network with professionals and to showcase an individual's talents and experiences. The problem is that the LinkedIn community often lists too much information about an organization that they are or have worked for. To validate this concept, a random listing was pulled from LinkedIn from the profile of a network administrator. For security reason, the person's name and the company in which they work for will not be displayed in the image. The information should always be approached from an attacker's perspective to determine if it holds any value for an attack.


My role consists of a number of responsibilities including:

- Managing and supporting Cisco Call Manager v10.x with over 1100 end point devices
- Windows 2008/2012 AD Servers administration and support
- VMware 5.1 with over 280 VMs
- Cisco UCS Blade Systems
- Cisco Nexus 7K
- Cisco Catalyst 2960, 3750-X, 3850
- Cisco ASA Firewall 5520 & 5585-X with IPS
- Palo-Alto Firewall
- VPN Gateways
- Cisco ASR Routers
- 130+ Cisco Voice Gateways (2900 & 3900 series)
- WLC Wireless Controller with 150+ APs
- Cisco WAAS infrastructure
- Security Hardening
- Cisco NAC / Cisco ISE (Identify Services Engine)
- General IP Network Management
- Projects covering network maintenance & expansion
- BAU activities
- Working with a great team managing and supporting hundreds of clients and remote sites

Figure 5: System engineer LinkedIn post

The first thing that an attacker would notice is that the network has a combination of Cisco and Palo-Alto products. Not only did this individual mention that they are using Cisco devices, but they also told the models which are deployed. Such information smooth's the path for the attacker. Anyone looking to penetrate this company can search for vulnerabilities against the listed model types. As a proof of concept, I have listed vulnerabilities against the Cisco Catalyst 3750-X device mentioned in the listing (CVE details, n.d.).

Cisco » Catalyst 3750-x » : Security Vulnerabilities

Cpe Name:*cpe:/h:cisco:catalyst_3750-x*

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
1	CVE-2013-5522	264		+Priv	2013-10-24	2013-10-25	6.8	None	Local

Cisco IOS on Catalyst 3750X switches has default Service Module credentials, which makes it easier for local users to gain privileges via a Se

2	CVE-2012-1338	362		DoS	2012-08-06	2013-04-01	6.3	None	Remote

Cisco IOS 15.0 and 15.1 on Catalyst 3560 and 3750 series switches allows remote authenticated users to cause a denial of service (device rel CSCts88664.

Total number of vulnerabilities : **2** Page : 1 (This Page)

Figure 6: Cisco vulnerability

2.3 Information from Websites

The social media sites used today can provide a wealth of information. However, it may be difficult to find information about several accounts owned by an individual. Websites such as namechk.com can resolve this issue. Instead of checking against one social media website, namechk runs a query against many of the traditional media and communication domains used today (namechk, n.d.). The dashboard can they be used to connect to the existing page if the account does exist. One additional feature of the website is the ability to use email addresses as well as nicknames used by an individual. Figure seven shows a search against accounts that use the name 'Hacker'.

Jose Ramos, joseramostrd@gmail.com

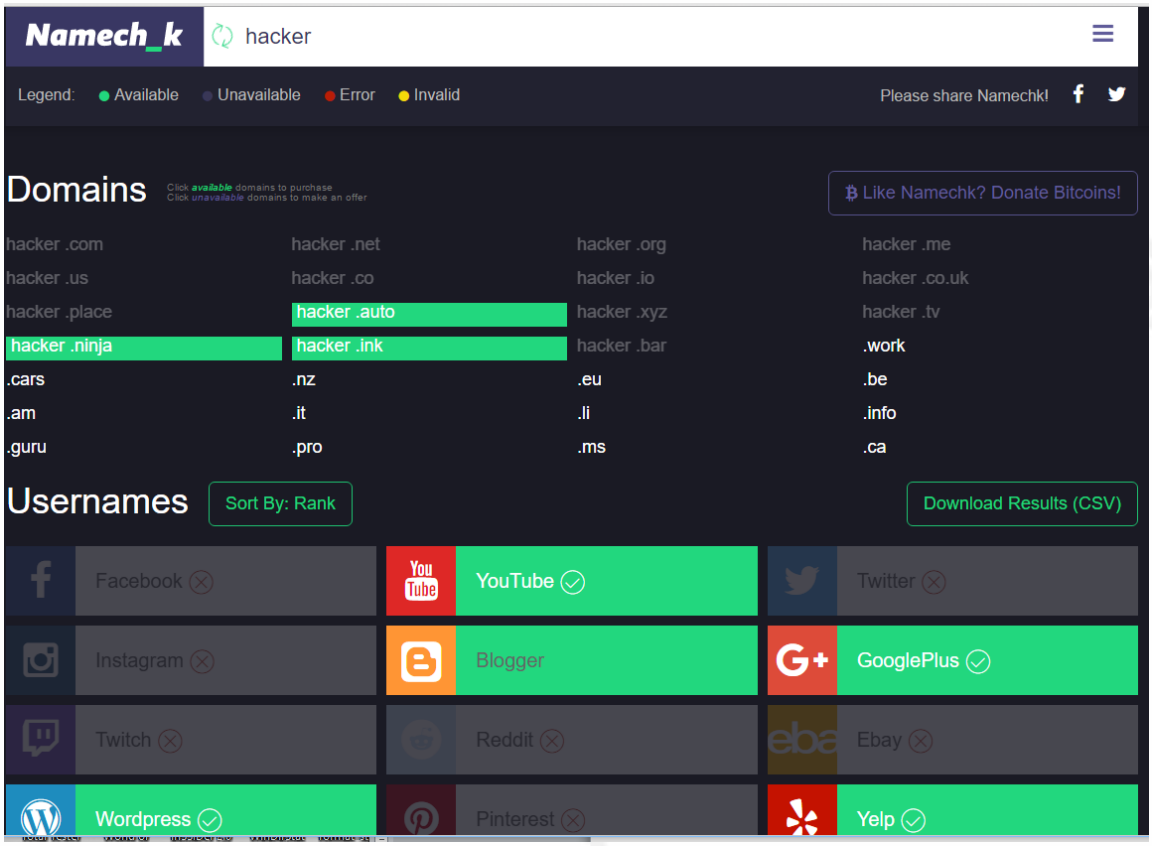


Figure 7: Namechk website

Our country has seen their fair share of data breaches. In many data breaches, the information is either sold off or posted on the Internet for everyone to see. Many of the companies send a notification alerting individuals of the breach and then recommend that they change their password. While this does correct the issue with the current website, it doesn't change the fact that people use the same password across many sites. An attacker can easily pull find account information from a breach on a paste site and then replay that information into a different account that they discovered by using namechk.com. To put things into perspective, an image from informationisbeautifiul.net is shown below. The website shows an informational timeline of breaches over the past decade. Look at each of these breaches and visualize a complete database of information being dumped on the Internet.

Jose Ramos, joseramostrd@gmail.com

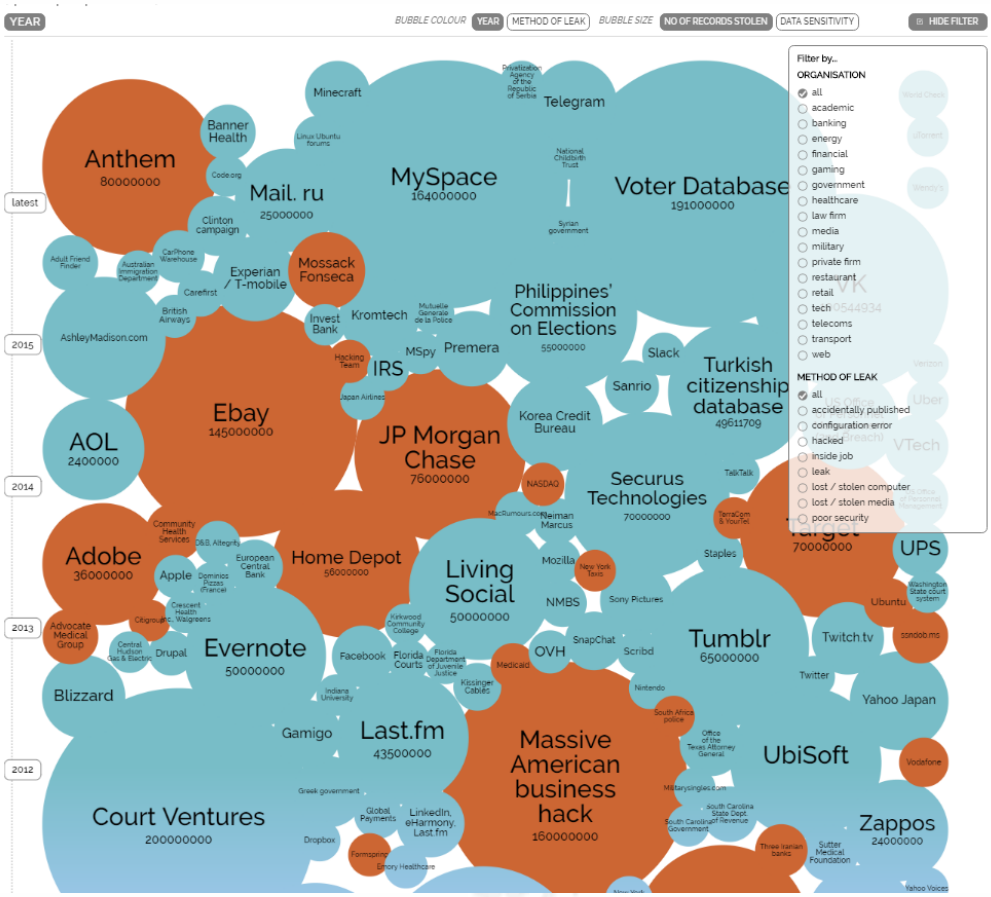


Figure 8: A Decade of Breaches

As one would imagine, anything that is used for good can be used for evil. People are concerned about these breaches and would like to know if their information has been posted on the Internet. A website has been developed to assist with this very need. The website checks to see if your email address was part of a breach and also crawls paste sites to view if your credentials have been posted (Have I been pwned, n.d.). The site is called haveibeenpwned.com and sounds like a lifesaver, right? Wrong, an attacker would use such a website for the very opposite reason. Someone seeking a password can plug the email address of their victim into the website to see if their credentials have been compromised. If confirmed, they can then navigate to the paste site to gather the credentials and attempt to enumerate the account. Figure nine shows a query against a Gmail account named "johndoe." The website responded with results stating that the email has been seen in 31 breaches and found in over 29 paste sites.

Jose Ramos, joseramostrd@gmail.com

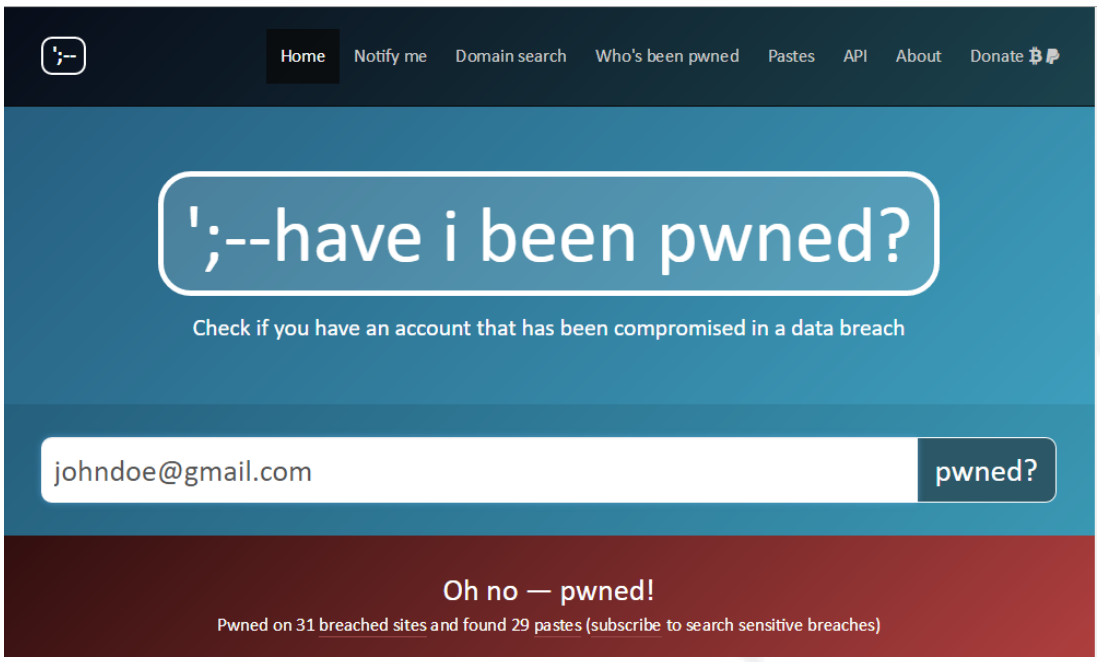


Figure 9: Have I been pwned

2.4 The Toolbox

Using Internet web browsers and websites to find information are great ways to seek information. However, many tools have been created to automate the manual discovery of information. The Kali Linux suite is a security distribution that houses some tools that can be used to enumerate both networks and people. In this section, we will go over a few of these tools and discuss their functionality.

One of the most powerful information gather tools in the Kali distribution is Maltego created by Paterva. The tool can enumerate information on both networks and individuals. Maltego comes in three different flavors the Community Edition (free and included in Kali), Maltego Classic, and Maltego XL. All three of the flavors work similarly; however, the paid versions carry additional options. The image below illustrates the value Maltego adds to the information gathering process.

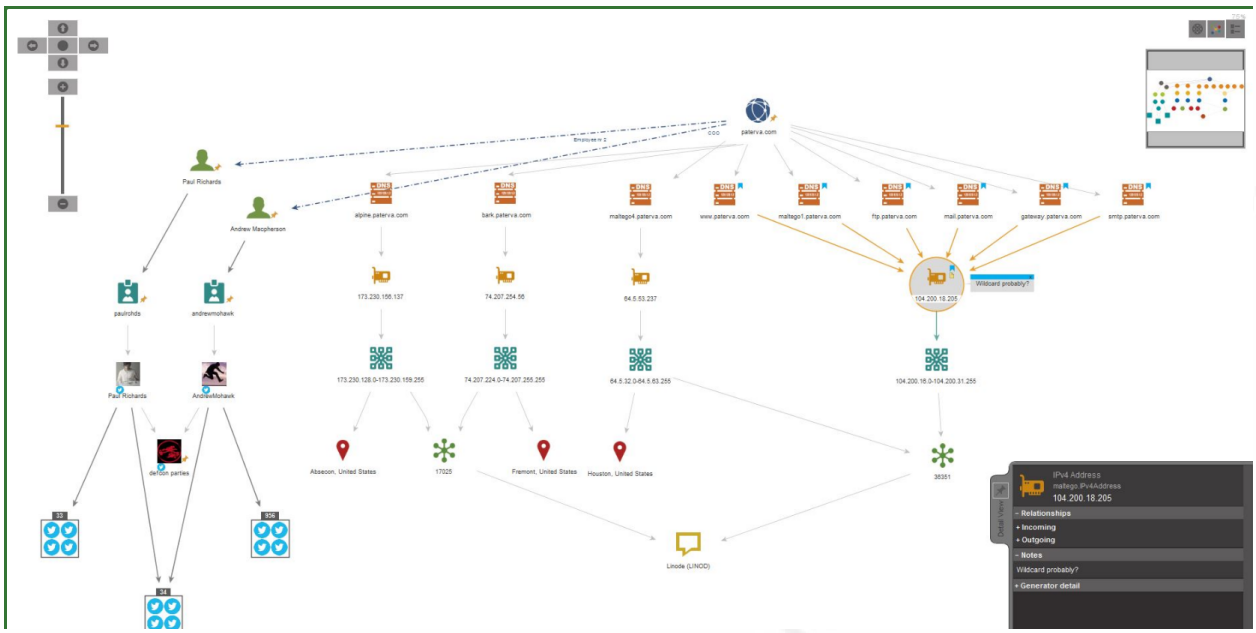


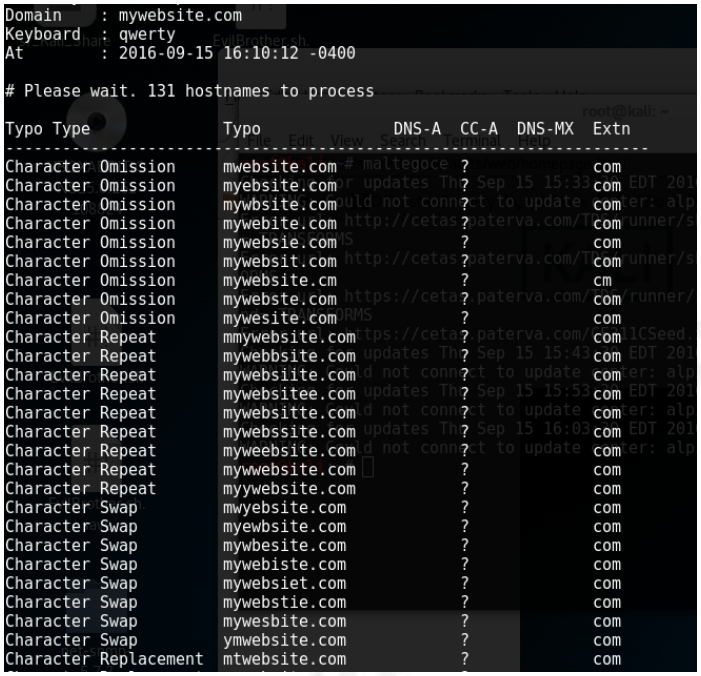
Figure 10: Maltego graph

The Maltego graph is the workspace that is used within the tool. Figure ten starts with the domain and then continues to branch down as it discovers information. One of the greatest features of this tool is that you can start from any item (i.e. person, domain, account, or IP address). Starting from paterva.com, the attacker was able to enumerate the DNS servers related to the domain. Further enumeration identified employees and network addresses connected to the DNS servers. This tool allows an attacker to connect the dots on a visual graph in real time. Furthermore, emails that are found can be viewed on the console itself. One of the caveats about Maltego is that it gathers information from various sources based on your search criteria. In the event you go beyond the target range, you may start to intercept data that does not pertain to the target at hand. For example, if you are checking for a user by email address, you might come across a secondary person that was copied on the message. The secondary email address of the individual may lead you to a domain that does not have any relevance to the initial target being investigated. They say that on the Internet we are all connected; this tool shows just how interconnected we are.

Another useful information tool found in the Kali distribution is The Harvester. This tool allows an attacker to input a company or domain name and cross reference the information across known data sources such as Google, Bing, and LinkedIn. A search for Yahoo.com against a LinkedIn database will provide results of individuals on LinkedIn who have listed Yahoo as their employer. The list can then be exported and

used in additional attack strategies against a targeted network. The Harvester is a simple text-based tool that takes the footwork out of finding employees at a particular company. The best part of this tool is that it can search and provide results in seconds.

Urlcrazy is another tool that is incorporated into the Kali distribution. This tool allows for an attacker to view all registered variations of a domain name. For example, let's say that we own a domain called mywebsite.com. Urlcrazy will display any related domains to the one I typed. Figure eleven shows results on this query.



```
Domain    : mywebsite.com
Keyboard  : qwerty
At        : 2016-09-15 16:10:12 -0400

# Please wait. 131 hostnames to process

Typo Type            Typo              DNS-A  CC-A  DNS-MX  Extn
-------------------------------------------------------------------
Character Omission   mwebsite.com      ?              com
Character Omission   myebsite.com      ?              com
Character Omission   mywbsite.com      ?              com
Character Omission   mywebite.com      ?              com
Character Omission   mywebsie.com      ?              com
Character Omission   mywebsit.com      ?              com
Character Omission   mywebsite.cm      ?              cm
Character Omission   mywebste.com      ?              com
Character Omission   mywesite.com      ?              com
Character Repeat     mmywebsite.com    ?              com
Character Repeat     mywebbsite.com    ?              com
Character Repeat     mywebsiite.com    ?              com
Character Repeat     mywebsitee.com    ?              com
Character Repeat     mywebsitte.com    ?              com
Character Repeat     mywebssite.com    ?              com
Character Repeat     myweebsite.com    ?              com
Character Repeat     mywwebsite.com    ?              com
Character Repeat     myywebsite.com    ?              com
Character Swap       mwyebsite.com     ?              com
Character Swap       myewbsite.com     ?              com
Character Swap       mywbesite.com     ?              com
Character Swap       mywebiste.com     ?              com
Character Swap       mywebsiet.com     ?              com
Character Swap       mywebstie.com     ?              com
Character Swap       mywesbite.com     ?              com
Character Swap       ymwebsite.com     ?              com
Character Replacement mtwebsite.com    ?              com
```

Figure 11: Urlcrazy results

The tool provides results on character omissions, repeated characters, additional characters, as well as swapped and replaced characters. An attacker can use this information in the attempt to identify mail servers (mail.mywebsite.com) and other servers that are related to the targeted network. In addition to seeing what is available, an attacker can also register a similar domain to use for spam against the target organization. It wouldn't be too difficult to register mywebste.com (removing the "l") and sending an email posing as an administrator requesting a user's password for system maintenance. It is very common for the human eye to overlook such changes, especially when it is a busy day and they have hundreds of emails in their inbox.

2.5 Defense and Identification

Jose Ramos, joseramostrd@gmail.com

We have seen how easy it is for an attacker to gather information. The best method to protect your information is by limiting how much information is publically posted on the Internet. In cases with social media, it is essential for individuals to know where they are posting the information and that privacy settings are configured. A corporation can have a bit more responsibility, especially when dealing with client side information. In such cases, a company must make sure that to protect their client's information in transit and at rest.

It is easy to assume that someone is in your network viewing and extracting information. However, tools such as Wireshark can assist in viewing your network traffic and evaluating how machines are communicating on the network. Once again, a clear understanding of networks will be needed to view and analyze the Wireshark traffic. This tool can show source and destination address and the protocols that were used across the network. Let's take this into perspective. If you see that your one of the machines on the network has been transferring data to an IP address in China via FTP every night at 2:00 am, this should something to look into.

The traffic on a Wireshark capture can be filtered to narrow down to specific information. For demonstration purposes, I have filtered the traffic capture on my network to view data going from one machine to another. The "ip.src" command represents the source address, and the "ip.dst" shows the destination address. As mentioned, if traffic is being sent to a foreign location that is unintended, it is not a mistake. Such a threat should be looked into.

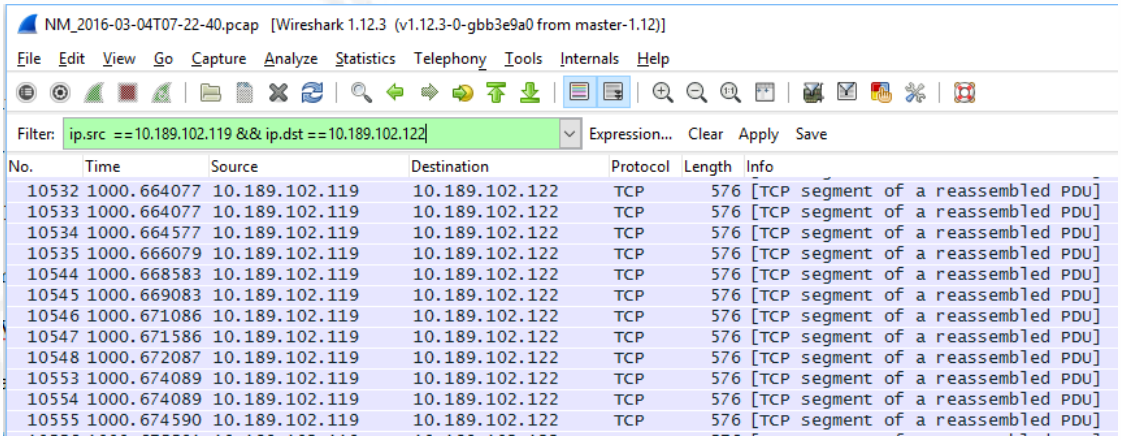


Figure 12: Wireshark capture

Wireshark is a great tool when used for good. In addition to seeing a source and destination, the tool can also capture messages in clear text when secure data transfer

methods are not used. The below image shows a capture of traffic from an HTTP (not secure session). This particular message has little use for an attacker; however, account ID's and passwords can also be captured via the same method.

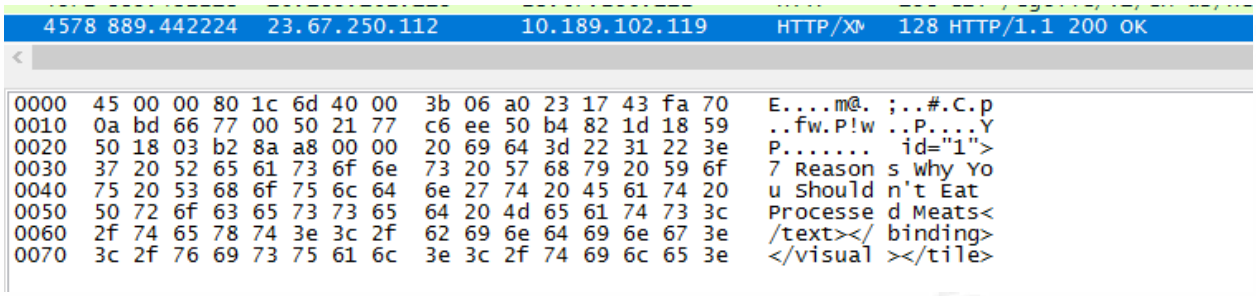


Figure 13: Clear text Information

Coffee shops and airports are huge targets for these types of attacks. Attackers often spin up free Wireless access points in these locations to perform such an information enumeration attack. Once the client connects to the network, the attacker can stand in the middle of the Internet connection and the client. This attack is commonly referred to as a man in the middle attack. Since the attacker is the middle man, they can virtually view the traffic going to and from the server. Also, the attacker can then use tools such as SSL strip to remove the security of a protocol like HTTPS and still view the traffic going across the wire. The best defense against this type of attack is not to connect to networks that you do not know. In the event the connection is a must, a VPN connection should first be established.

2.6 Putting it all Together

The truth is information cannot be gathered using one tool or resource. To efficiently collect information on a targeted network or person, multiple resources need to be used. This paper was meant to expose the reader to the various sources information can be gathered, but the format was intentionally written to bounce back and forth between network and person to simulate an actual investigation. Many times information on an individual is needed to further enumerate a network and vice versa.

It is essential to validate information when it is being gathered. Incorrect subnets and not reviewing the received information can lead the investigation off on a wild goose

chase. Knowing what you are looking for and where to find it will always save time during an investigation. One may choose to manually search LinkedIn for hours finding Yahoo employees, whereas people who read this paper may use The Harvester. There is no simple way to locate the information one might be seeking; but with enough patience and dedication, they are bound to find results.

3. The Closing Act

We have discussed a wealth of information in this paper. The discussions ranged from attackers gaining information when our guard is down, to using tools and attack methods to gather the information ourselves. When it comes to information gathering, it is important to understand both sides of the playing field. A wise man once said the best way to catch a criminal is to think like one. This is a concept that we should keep deer to ourselves when attempting to protect our information. If you take anything away from this paper, it should be that attackers are very crafty and can be very persistent when it comes to achieving their goal. For this reason, alone, we should always keep a defense in depth mindset and also exercise information awareness to our friends and families. One last recommendation would be to use to tools and techniques that were discussed to find out what information is available about you on the Internet. You may find some accounts opened in your name, or even personal information easily accessible. Just remember if there is a will, there is a way. Our information is out there just waiting to be found. Some may call it data; but in the end, this is the information that we seek.

Jose Ramos, joseramostrd@gmail.com

References

Combs, G. (n.d.). *About Wireshark*. Retrieved October 3,2016, from http://www.wireshark.org/about.html

CVE details. (n.d.). *The ultimate security vulnerability datasource.* Retrieved September 20, 2016, from https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-22747/version_id-130969/Cisco-Catalyst-3750-x-.html

Exploit Database. (2009). *Google hacking database.* Retrieved September 20, 2016, from https://www.exploit-db.com/google-hacking-database/

Have I been pwned*. Have I been pwned?* (n.d.). Retrieved September 19, 2016, from https://haveibeenpwned.com/

Information is Beautiful*.* (2016). *World's biggest data breaches*. Retrieved September 21, 2016, from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Kaplan, H. (2015*). Lua/Dissectors - The Wireshark Wiki*. Retrieved October 3, 2016, from https://wiki.wireshark.org/Lua/Dissectors

Microsoft. (n.d.). *Address Classes.* Retrieved September 19, 2016, from https://technet.microsoft.com/en-us/library/cc940018.aspx

Microsoft. (n.d.). *Public and private addresses*. Retrieved September 19, 2016, from https://technet.microsoft.com/en-us/library/cc958825.aspx

SANS. (n.d.). *Google hacking and defense cheat sheet.* September 20, 2016, Retrieved from https://www.sans.org/security-resources/GoogleCheatSheet.pdf

Verizon.(2016). 2016 Data Breach Investigation Report. Retrieved October 4, 2016 from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Jose Ramos, joseramostrd@gmail.com

Jose Ramos, joseramostrd@gmail.com