INFORMATION GATHERING

Compiled by

Dr. K. Buchiraju
Dean Placements

Dr. K.V.S.Raju
Dean Training, GRIET

Dr. T. Jagannadha Swamy
Dean Career Guidance, GRIET

GOKARAJU RANGARAJU
Institute of Engineering and Technology
(Autonomous)

Griet SKILL SERIES

INFORMATION GATHERING

Compiled by

Dr. K. Buchiraju

Dean Placements

Dr. K.V.S.Raju

Dean Training, GRIET

Dr. T. Jagannadha Swamy

Dean Career Guidance, GRIET

"Information is power," as the saying goes. And in most scenarios it's true: having critical information, at the right time, and especially knowing how to use it, can be a great source of power.

In the **cybersecurity** world, the security data about any target (person, company, domain name or service) is something that's coveted by parties on all fronts, including red teams and blue teams.

Therefore, mastering the information gathering process is one of the ultimate goals of any cybersecurity researcher. That's why today we'll be exploring the main information gathering concept, as well as some information gathering techniques and tools that will help you boost your daily infosec tasks.

What's information gathering?

When it comes to getting a clear information gathering concept, the simplest way to define it would be the process of collecting information about something you are interested in.

For those in the cybersecurity industry, this is the first step to take during the earlier stages of any hacking activity (both cracking and ethical hacking), when any black- or white-hat researcher needs to gain as much information as possible about the desired target.

While it's a fun activity for some researchers, information gathering is also one of the most time-consuming tasks during the intel-recon process, and that is why time management is so important.

What are the objectives of information gathering in cybersecurity?

Any basic cybersecurity information gathering process often includes these two types of data collection goals:

1. Collecting network data: Such as public, private and associated domain names, network hosts, public and private IP blocks, routing tables, TCP and UDP running services, SSL certificates, open ports and more.

2. Collecting system-related information: This includes user enumeration, system groups, OS hostnames, OS system type (probably by fingerprinting), system banners (as seen in the banner grabbing blog post), etc.
But there's a lot more involved. Let's learn about it, by exploring the most popular techniques used during this phase.

Information gathering techniques

Ethical hackers use a big variety of techniques and tools to get this precious information about their targets, as well as locations and data collection software they'll be using towards the information gathering goal.

How to gather information?

- **Social engineering:** This includes in-person chat, phone conversations and email spoofing attacks. What all these methods have in common is the psychology of human weakness, needed to get maximum data about the target.
- **Search engines:** Web crawlers can be used to fetch information about anything, and this includes companies, persons, services, and even real hacks, as seen in our previous article about Google Hacking.
- **Social networks:** Facebook, Twitter, LinkedIn and other social networks are great sources of information to build a profile, especially when targeting individuals.

- **Domain names:** These are registered by organizations, governments, public and private agencies, and people. Therefore, they're a great starting point when you want to investigate someone. Personal information, associated domains, projects, services and technologies can be found by inspecting domain name information.
- **Internet servers:** authoritative DNS servers are a great source of information, as they often include every single surface point exposed to the Internet—which means a direct link to related services such as HTTP, email, etc. In our previous article about passive DNS, we analyzed the importance of DNS servers, and especially passive DNS-recon services, such as the ones we offer here at Security Trails.

All these techniques are really useful when combined with enterprise security tools. Keep reading to discover how to maximize your information gathering results by using some really cool infosec utilities.

Information gathering tools

There are a lot of tools to discuss when talking about information gathering, including one particular software we can't avoid mentioning...that's Kali Linux, one of the most popular cyber security linux distributions around.

We've written about the top Kali Linux tools before, but that was a general review of the most popular tools on that Linux distro. When it comes to information gathering, Kali Linux includes one of the biggest collections ever. To be precise, exactly 67 information gathering utilities will help you get all the valuable data you need during your infosec investigations.

Creating a full list of all the information gathering tools available would be monumental, not to mention difficult. That's why we've created a summary of the top 10 most popular tools that, in our experience, may help you during your information gathering process:

1. Nmap: Our beloved network scanner will be always in the #1 position when it comes to data gathering tools. It can be used not only to scan ports and service fingerprinting, but also as a DNS enumeration and network mapping tool.

2. Unicornscan: Combined with Nmap, it can give you the complete picture of any remote network or host, as it is able to perform asynchronous stateless TCP scanning with all variations of TCP flags, as well as TCP banner grabbing, async UDP Scanning, OS fingerprinting, and much more.

3. Sublist3r: This is one of the best subdomain enumeration tools around, one that will help you create a virtual subdomain map of any website in no time. By using Google dorks and other search engines such as Baidu, Ask, Yahoo or Bing, it can also be used to perform a brute force subdomain discovery attack with wordlists, thanks to its subroute integration.

4. DMitry: Its name stands for Deep magic Information Gathering Tool, and is one of the top terminal-based tools when it comes to intel reconnaissance tasks. It will allow you to get any available data from any host, such as subdomains, email addresses, open ports, WHOIS lookups, server data, and more.

5. Th3inspector: This infosec utility will enable you to fetch all kinds of website-related information, such as page data, phone number, ip addresses of HTTP and email server, perform a domain WHOIS lookup, bypass the Cloudflare proxy, check the age of your domain name, scan remote active services, subdomain mapping, and even work as a CMS detector.

6. Devploit: This tool is used to extract DNS and domain data, including DNS lookups, WHOIS lookup information, reverse IP info, port scanning, DNS zone transfer, HTTP-headers, GEOIP lookup, subnet lookup, etc.

7. Bettercap: Known as the swiss army knife for networking, it's used mostly for network recon and information gathering, especially for WiFi, Bluetooth low energy devices and Ethernet networks.

8. Traceroute: As one of the most popular network tools used to track the path of networks packets between one IP address to another, it's a powerful recon tool that will let you gain critical network information about IP addresses and networking routes.

9. WHOIS: The WHOIS command is a great source of data for fetching domain- and IP-related information, including tech and admin names, telephones, addresses, country, DNS servers, etc.

10.Dig: Whenever you need to find current data about DNS records, Dig is one of the best tools there is to help you to accomplish that
task, whether you want to get A, NS, TXT or CNAME records.

What's the best way to gather information about any company?

Most of the tools we've mentioned are terminal-based, and while those are good solutions for the console geeks, even some advanced IT users need to jump into web-based tools from time to time. Most importantly, you might need an AIO solution that can not only give you isolated results, but also help you correlate all the information, to ultimately generate a threat intelligence report that includes all the critical data.

Let's see how SurfaceBrowser™ can help you gather information about any company in the world. In this information gathering example, we'll be using hp.com domain name to see what information we can get.

What's the best way to gather information about any company?

Most of the tools we've mentioned are terminal-based, and while those are good solutions for the console geeks, even some advanced IT users need to jump into web-based tools from time to time. Most importantly, you might need an AIO solution that can not only give you isolated results, but also help you correlate all the information, to ultimately generate a threat intelligence report that includes all the critical data.

Let's see how SurfaceBrowser™ can help you gather information about any company in the world. In this information gathering example, we'll be using hp.com domain name to see what information we can get.

Once you login into the main interface, you'll notice a summary of all the information available for that domain name, in this case:

- IP Addresses (1,069)
- All domains related to HP (1,503)
- Subdomains (178,131)
- Reverse DNS entries (38,342)
- SSL Certificates (13,823)
- Whois contact information
- Current DNS records
- DNS history

When we move to the IP Addresses area, we find extensive information regarding the IPs, including Summary by Regional Registrar, Stats by IP subnet size, as well as the full list of IPs filtered by number of IPs blocks, IP Count, Unique User Agents, RIR, Hostnames and number of hosted domain names, as shown below:

From that IP list, you'll be able to jump into full IP block information, hosted domain names and domains associated with that IP block.

By clicking any of the IP blocks in the list, you'll find interesting network information such as: IP Count, Bitmask, Base IP, Broadcast IP, Mask, Host Mask, as well as Neighboring IPs. When it comes to the Service Provider, we provide accurate data including ASN, Organization and registered company name:

Regarding Domain information, the DNS records option will enable you to get the full list of A, AAAA, MX, NS, SOA and TXT records, as seen in the following screenshot:

But what if you need to check out the DNS history for the domain name? No problem, we got you covered! Our DNS historical records include full information about past records including A, AAAA, MX, NS, SOA and TXT; also in order of IP Addresses, Organization, First Seen, Last Seen and Duration Seen:

In regards to subdomain enumeration, we offer the best results you'll ever get, and this includes the full list of subdomains and a useful dashboard where you can tweak the information you want right before your eyes, including summaries of:

- Subdomains by Hosting Company
- Subdomains by IP
- Subdomains ordered by Open Ports

For example, if you want to filter all subdomains by their Open Ports, it's easily performed by selecting the ports you want to see, then checking the results. You'll see something similar to this:

Yay! We were able to get critical open port information about hp and all its subdomains in only a second, including ports such as 21, 22, 80, 443, 990, 6379 and 29200.

PTR records are a great source of information, too. They can help you catch bad guys in the act of malicious campaigns, as covered in our previous article: How to use reverse DNS records to identify mass scanners.

If you want to discover the full PTR data from the hp.com domain name, we present this information including full PTR summaries by Open Ports, as well as by Similar Records, which will yield the full PTR data by Record, Open Ports and the number of associated IP Addresses:

Another great source is the traditional WHOIS information behind any domain name. In this case, our WhoWasTM Smart WHOIS history feature will show you any present and previous WHOIS records without the interference of annoying privacy guard filters.

Click on any part of the timeline to get instant access to WHOIS information such as Domain Registrar Information, WHOIS Registrant, Admin Contact, or Technical Contact:

Now what about SSL certificates? SurfaceBrowser™ offers an excellent way to extract SSL data from any website, and integrate it with the rest of the intel we already have about the domain names and subdomains. All of this magic happens when you click the 'Certificates' option, which will let you choose

different summary options, such as: Summary by Company, Summary by Creation Year, Summary by Expiration Year and Summary by Validity.

Let's say, for example, that you want to easily detect which certificates are expiring next year. You can use the 'Summary by Expiration Year' feature and get results in less than a second:

All of these features make SurfaceBrowser™ one of the top threat intelligence tools around.

Summary

Information gathering is just one of the initial steps taken during most infosec investigations, and there are many ways to do it, with different techniques and tools. While conducting research on any target, you'll be surprised at how much data you get about the host or domain name you are investigating.

Sometimes you'll find a lot of relevant information, on other occasions you'll come up with useless data, and,

still, in other scenarios there will be a mix—good data and mere noise combined. Collecting all this data takes time, and piecing together the different pieces of cybersecurity trails you get, cleaning all the garbage, and getting only the useful and critical parts can be even harder...but don't worry, that's why we're here to help you.

SurfaceBrowser™™ is one of the best recon tools available to help you discover, pivot through and extract all the data, all in one single place. It's the perfect way to boost your data reconnaissance and threat intelligence tasks. Book a demo with our sales team today!

GOKARAJU RANGARAJU

Institute of Engineering and Technology

(Autonomous)

Bachupally, Kukatpally, Hyderabad - 500 090, INDIA
Ph : 072077 14441 www.griet.ac.in