

PASSIVE RECONNAISSANCE



**Northeastern
University**

Name: Davindernain Singh Sehgal

NUID:



Table of Contents

Sr.no	Title	Page no.
1.	Executive Summary and Organization Details	3
2.	Tool 1: Spiderfoot	4
3.	Tool 2: Maltego	4
4.	Tool 3: Dig	5
5.	Tool 4: Shodan	5
6.	Tool 5: Virustotal	6
7.	Tool 6: DNS dumpster	6
8.	Tool 7: Wappalyzer	7
9.	Tool 8: Whois Lookup	8

Executive Summary:

Reconnaissance is the technique used to gain intelligence and knowledge about a target and is considered to be the first step for various data hacking procedures and also for penetration testing. Reconnaissance helps you get data on a victim machine which helps you understand what you're dealing with so that you can make informed decisions on how to proceed with a cyber attack. It can help you get important information on the target such as their open ports, registered domains, certificates, and devices they use. In simpler terms, Reconnaissance is the process of collecting Intelligence about the vulnerabilities their system holds and is also publicly available.

Organization Chosen:

www.thesouledstore.com

The Souled Store is an online store based in Mumbai, India and it was founded in 2013. TheSouledStore is actually a place where all kinds of fans get the merchandise of their favorite TV shows, movies, Cricket teams, Cartoons, Anime, and others. Although they sell their products all over India, they are still a tiny team that consists of some college students who just wanted to do something new.

I chose this organization because I've bought products from this site and also I like how much they are able to do with a small team in their hand. They recently crossed the 3 million customer mark and I feel that this is a medium-sized organization that would be perfect for my reconnaissance assignment. You can either shop by Theme or product, and they have a very wide range of both of them.

TOOLS

1. Spiderfoot:

Spiderfoot is an open-source (free for anyone and everyone to use) intelligence tool that scans a given target website from a plethora of perspectives such as the domains owned by the target, their email addresses, DNS server information, SSL certificates, etc.

Like most OSINT(Open Source Intelligence) tools, Spiderfoot goes through the entire internet and looks at publicly available data related to the target and then not only lists it but also provides graphical illustrations of the same to understand the reconnaissance data extracted.

One of the most prominent features of this tool is to extract all the domains used by the target and an attacker can use this information including the others he has been able to extract to perform a sort of phishing attack that would redirect traffic to a different domain that may look similar to the actual domain. This can end up fooling clients and can lead to a data breach which puts the client at risk.

Controls: Updating certificates and software with the latest patches as well as a strong firewall in the network design can help prevent this attack and the potential attack that may follow in the future while also protecting their clients.

2. Maltego:

Maltego is an inbuilt tool that comes with Kali Linux distribution. It is easy to use and it very simply organizes the intelligence gathered in a clean report which makes it easier to read and navigate through. Maltego not only creates diagrams, but also tables to list out all the entities connected to the target domain such as servers, databases, DNS names, Phone numbers, etc. An interesting thing that Maltego does is that it shows a snapshot of your target and tells you exactly when the last snapshot of the same domain was taken using Maltego.

After running Maltego on the target, I found out that this domain has around 66 entities and 69 links that Maltego was able to find. Including 5 email addresses, 13 domains, 10 phone numbers, and other details. I think that finding domains related to a website might not be as big a deal, as finding out email addresses and phone numbers. The snapshot that Maltego shows has been removed from the site itself but these snapshots are dated back to 2014-2015. This could mean that the organization had put up security measures that

have since then made it difficult for Maltego to take snapshots or that no one has looked up this domain using Maltego.

If an attacker were to gain this knowledge and knows enough about how network architecture works and plots out a few flaws on the website, using the information gained such as phone numbers and email addresses, they can potentially break into the system to get out sensitive data from the organization.

Controls: The most practical way I think can be implemented to save this organization from such attacks is by implementing MFA into the system and using it to avoid being broken into using the email addresses and phone numbers available publicly which I believe are of the employees of the target organization.

3. Dig:

Dig is a command line-based passive recon tool built inside Kali Linux that is used in network administration to check and look up DNS(Domain Name Server). Dig gives you server information including the version of OS being used and their server IP address too. Although this tool isn't as powerful as others on the list, it is useful for a small and quick recon. I was able to find a very important piece of information using Dig that the server is using Debian 9.18.0-2.

If an attacker were to get hold of this information, they would first look for known vulnerabilities in that version of Debian and see if they can exploit those vulnerabilities and break into the said server to extract potentially sensitive data.

Control: The easiest way for an organization to prevent such an attack would be to have more than one single server that is updated and patched regularly by the network security team. A backup server must be added in case an attack were to happen and firewalls must be placed into the network architecture so that even if the attacker has enough information on the DNS servers, it is still hard to exploit the information.

4. Shodan:

Shodan is one of the most popular OSINT Passive reconnaissance tools that reveals the ports used by the target domain, the web technologies used, protocol versions, and SSL/TLS versions. Usually, Shodan is also known to reveal known vulnerabilities that the system may have by looking at the exact version of the software or hardware being used.

I was able to find out the version numbers of the SSL/TLS version and the protocol version too. If an attacker were to get hold of this, they would first find out if those specific versions are known to have any vulnerabilities. If they do, they will know where to begin.

Control: This control method is repetitive but also the easiest yet missed out method, which is to keep the latest version of all software, you've got running on your organization because the new version has patched the already known bugs of the past versions. Using an older version of a given software deliberately is an invitation to network-based attacks.

5. Virustotal:

Virustotal can be best described as an online antivirus tool made for websites that not only collaborate with a lot of leading antivirus software but used all their knowledge of known viruses, vulnerabilities, and tools to run a complete scan on the target domain. This tool is very popular because rather than checking up with a few antivirus software and missing out on important information that could lead to a potential data breach, Virustotal does the whole job for you and lets you know if the target domain is malicious or not if it has ever been flagged, and if a virus is detected, it also tells the virus it detected and has a potential of harming the target.

If a given domain is flagged by multiple antivirus software on Virustotal, it could mean that some malicious content is present on the said target that should be looked into and taken care of. Although The last virus total, for www.thesouledstore.com, was less than a month ago and it has checked out to be clean, if a virus would have been found, an attacker could use that information to potentially create threats that revolved around bypassing that particular vulnerability.

Control: Like the souled store, all organizations should keep a thorough check on viruses and vulnerabilities that can lead to a breach into their systems. I would like to believe that the scan that happened less than a month ago was performed by an employee of the organization which is why not even one red flag was seen.

6. DNS Dumpster:

DNS dumpster is an online reconnaissance tool and its primary objective is to search the internet for similar domain names which determines if internet traffic can be redirected to another site instead of the actual one to perform a phishing attack. DNS dumpster is also

useful to list out the DNS servers allotted to the website including their geographical location on the world map as well as their IP addresses.

An attacker can use this hostname information in planning his phishing attack. For example: A user might think that they are on the actual souledstore website but they are actually on a site that looks similar to the original one. They may end up logging in using their credentials but not be able to log in. They then just go back, enter the site URL and reach the actual site and log in there and continue with their normal shopping. But amidst all of this, the attacker already has their information and credentials which he may then use.

Control: Generating certificates from a known CA (Certificate Authenticator) is the first and the simplest way to secure your website and let your clients know which website is actually secure and which isn't.

7. Wappalyzer

Wappalyzer is an open-source reconnaissance tool that acts as a website technology lookup. This means that it tells you about what happens in the backend of a target domain, such as the Operating system used, web server, programming languages use, and also their respective versions.

For thesouledstore.com I was able to find out a lot of details including that it uses javascript which has two libraries and I was also able to find out their version numbers. I was able to find out the expiration date of the TLS certificate which is Aug 6 of 2022. I was also able to figure out how this organization advertises themselves.

If an attacker wants to either get into the main server of the target organization or do a simple phishing attack, all they need to do is figure out a vulnerability in the javascript libraries or advertise their phishing website on the same platforms they advertise, so as to bring genuine customers and risk their data.

Control: Updated Javascript libraries should be implemented in the module including a certificate generated for the website a few days prior to the expiration of the current one. This can help secure the said organization.

8. Whois Lookup

Whois lookup is another Online reconnaissance tool that gives you the information related to the certificate of the domain like other tools too, but also, it gives you information that shows the entity who registered the website (in this case: Godaddy).

According to whois lookup, it expires on 2025-11-30 while it was registered on 2012-11-30 and was updated on 2020-03-25. It also shows me the name servers, similar domains, and the complete registrar data.

We can see the location of the Addresses connected to it as well as the number of times it has been changed over the years. An attacker can use this information to potentially impersonate themselves as the registrar (GoDaddy) or also the client in this scenario. If the hacker has enough knowledge about certificates and it's working, they can extract sensitive information on the website and other entities attached to it with enough planning.

Control: To prevent such attacks, it would be best to keep updating your certificates from trusted registrars and CAs and keep shuffling between them as time progresses.