

Partial Passive Reconnaissance



**Northeastern
University**

Name: Davindernain Singh Sehgal

NUID: 

Target: Youthiyapa.com

Table of Contents:

Sr.no	Title	Page no
1.	Executive summary	3
2.	Tool 1: Spiderfoot	4
3.	Tool 2: Shodan	4
4.	Tool 3: Maltego	4
5.	Tool 4: VirusTotal	5
6.	Tool 5: Wappalyzer	5
7.	Tool 6: DNS Dumpster	6
8.	Tool 7: Dig	6
9.	Tool 8: Whois Lookup	6

Executive Summary:

Reconnaissance is a technique used by cybersecurity professionals to get useful and publicly available information about a given target to check for vulnerabilities in the target's system. This can be used for both good and bad purposes depending upon who this information is with. The reconnaissance technique is a very crucial technique for Network security because this helps you understand what domains, devices, certificates, and other important entities a target holds. In simple words, Reconnaissance is the process of gathering intelligence about the vulnerabilities of a system that is available publicly.

Organization Chosen:

www.youthiyapa.com

Youthiyapa.com is a merchandise website of one of the top YouTubers in India, [Bhuvan Bam](#). His youtube channel started exploding in 2016 and 2017 when his unique take on family comedy went viral all over the internet. Since then Bam has been able to maintain a large number of fan following who love to purchase merchandise from their favorite youtube content creator. The main office of youthiyapa.com is located in Delhi, India. Their merchandise includes everything from T-Shirts to hoodies to caps to facemasks to socks and more. This wide variety of product lineups is the reason for most of the online traffic experienced by this website. Although the reach of his channel is international, his office remains small and operated/managed by his close friends. This makes this website a perfect choice for passive reconnaissance as the team looking after the site is relatively small.

Tool: 1. Spiderfoot

Spiderfoot is an open-source (open for everyone to use) intelligence tool that scans a target from a variety of perspectives such as their email address, domains, DNS server, etc.

Basically, spider foot goes through the internet and looks at the publicly available information available about a target and then displays it in a list and a graph.

Like most other OSINT(Open source Intelligence) software, Spiderfoot list's all the domains you registered with the target and this can be used against the target.

The attacker can use this information to redirect traffic to a domain that is similar to the actual domain and take advantage of the clients.

Tool: 2. Shodan

Shodan is another OSINT tool that reveals the ports used by the domain, and the web technologies used but the main reason anyone would use Shodan to perform a passive reconnaissance is to figure out the vulnerabilities a system may have. Not all vulnerabilities are true, there are definitely false positives but the fact that some of these vulnerabilities are true, they can be all used against the target by an attacker.

The vulnerabilities listed are just based upon the version of the system and servers the target has, so it can be wrong sometimes as well. However, a cybersecurity professional can check all these vulnerabilities and possibly patch them so that these vulnerabilities are no longer viable and can't be exploited.

Vulnerabilities like such can be easily patched by either upgrading your system, upgrading your firewalls, or creating a different architecture.

Tool: 3 Maltego

Maltego is a tool that comes inbuilt with Kali Linux, it is fast and easy to use, not only that but also, this tool easily makes up a report for you that is easy to read and navigate through. Maltego easily creates a diagram of your domain connecting to different entities like servers, databases, etc.

Not only that, Maltego also shows a snapshot of the site you've targeted also with some additional information with a timestamp of when the site snapshot was taken.

If an attacker with enough knowledge about network architecture and network designs gets this information it would be easy for them to eventually figure out a way to exploit their design and break into the system to get out sensitive information finally.

Using Maltego I can see that this site has around 10 Maltego snapshots from 2017 and nothing after that, this site was created in 2017 itself. This tells that there is a chance that the creators of this domain ended up pen-testing it once when they created the site but haven't done it since. This is speculation, this can mean that I can try all the exploits of the system that were discovered after 2017, this gives the attacker an edge in getting sensitive information.

Tool: 4 VirusTotal

Virustotal is an online Reconnaissance tool that can be thought of as a tool that runs an antivirus scan on the domain and the systems attached to it that most antivirus systems might end up missing. The site puts up a list of viruses and sees if the target is affected by those viruses or not. It tells you if the Site on target is malicious or not and if the site has been flagged as malicious or not.

If a site ends up getting flagged by more than one antivirus software, this could mean that there is something fishy going on with the website which should be looked into. An attacker can use this VirusScan to his benefit because he can see if the system is vulnerable to a virus or not.

To defend against such attacks having an updated antivirus system on your servers and connected important devices is a must. Doing this will ensure the safety of your data and your client's data. This can also avoid data breaches.

Tool: 5 Wappalyzer

Wappalyzer is an online reconnaissance tool that tells you about the backend of a domain, such as the programming language used, the operating system used, their web servers, etc, and also their version of them. If an attacker lands up with this information he can figure out if there's an older version of the Operating system being used, an older version of a system means that there are a few vulnerabilities that haven't been patched and this can be exploited.

To defend against such attacks, having the latest version of OS and all software used in your architecture should be updated. Every update an exploit/weakness is found and patched making your system more and more secure.

Tool: 6 DNS Dumpster

DNS Dumpster is another online Reconnaissance tool and its main purpose is to search for related domain names to see if the internet traffic gets deflected to another malicious site or not. Not just that, DNSDumpster also lists the DNS servers allotted to the website including their IP addresses and rough geographical location.

An Attacker can use this hostname in planning his attack and proceeding with it. To defend against such an attacker having multiple hosts is a good idea as failure of one host on one location doesn't affect your website in the long term or sometimes at all. Unlike other DNS finding tools, this one searches up the normally hidden DNS so that a perfect Passive reconnaissance can be executed successfully.

Tool: 7 Dig

Dig is an inbuilt passive recon tool in Kali Linux, it gives you the name of the OS being used on the target's end including the version and their Server IP address. This tool isn't as powerful as others in the rooster, However, this is a small and quick reconnaissance tool.

An attacker can use the server IP address and the information that it basically runs on a Debian-based OS, he can exploit the vulnerabilities of the Debian OS.

The best way to get over such an attack is to have more than one main server and a complete backup server protected with firewalls with conditions such that even if an intruder has this information, it's practically useless.

Tool: 8. Whois Lookup

Whois Lookup is an online reconnaissance tool that gives you the certificate information about the domain like various other recon tools, but in addition to that, Whois Lookup gives you the information about who registered the website in this case (GoDaddy).

We can see the location of the IP address and how many times it has changed over the years. An attacker can use this information to get out information by either impersonating themselves as Godaddy or the client. With enough planning, an attacker can get sensitive information about the website and the other entities aligned with it.

To prevent such attacks, I would recommend updating your certificates after they expire but with different registrars.