Executive Post Graduate Certification in Cyber Security and Ethical Hacking

Assignment 02

Footprint a target using the OSINT Framework:

Here I am using theHarvester in Kali Linus for Gathering an Email List and my target is microsoft.com.

Here Target domain is microsoft.com and Search engine to use yahoo

theHarvester -d microsoft.com -l 200 -b yahoo

We found one email ID and 33 Host.

Again Target to different domain eccouncil.org and Search engine to use yahoo

theHarvester -d eccouncil.org -b yahoo

Here we found 4 mail ID's and 27 Host.

Gather DNS information using nslookup command line utility and online tool

Run cmd as administer and type nslookup for check the defult server

Set type=a, type as "a" configures nslookup to query for the IP address of a given domain and my target is www.intellipaat.com

```
C:\Windows\System32>nslookup
Default Server:  UnKnown
Address:  192.168.27.2

> set type=a
> www.intellipaat.com
Server:  UnKnown
Address:  192.168.27.2

Name:    www.intellipaat.com.localdomain
Address:  104.18.27.176
```

Here target domin DNS is 192.168.27.2 and www.intellipaat.com is resolving with 104.18.27.178.

Set type=cname

The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.

```
C:\Windows\System32>nslookup
Default Server:  UnKnown
Address:  192.168.27.2

> set type=cname
> intellipaat.com
Server:  UnKnown
Address:  192.168.27.2

DNS request timed out.
    timeout was 2 seconds.
intellipaat.com
        primary name server = june.ns.cloudflare.com
        responsible mail addr = dns.cloudflare.com
        serial  = 2364621607
        refresh = 10000 (2 hours 46 mins 40 secs)
        retry   = 2400 (40 mins)
        expire  = 604800 (7 days)
        default TTL = 1800 (30 mins)
>
```

Set type=a

Here we got the primary name server then we need to determine the IP address of the name server.

Set type=a

june.ns.cloudflare.com

```
> set type=a
> june.ns.cloudflare.com
Server:  UnKnown
Address:  192.168.27.2

Name:    june.ns.cloudflare.com.localdomain
Address:  108.162.192.176
```

Primary name server is store records associated with the domain.

Now, we can use an online tool NSLOOKUP to gather DNS information about the target domain.

http://www.kloth.net/services/nslookup.php

KLOTH.NET | Services | Radio | Internet | Software | Support | Aircraft | Links...

www.kloth.net > services > nslookup

NSLOOKUP: look up and find IP addresses in the DNS

Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.

This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.
This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.

NSlookup

Domain: ... the name of the machine to look up.

Server: localhost ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query: A (IPv4 address) Look it up

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page).
Basically, DNS maps domain names to IP addresses.
Although this web online service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver "localhost"/127.0.0.1.
To resolve an IP address by reverse lookup (get a computer's name if you only have its IP address), try to perform a PTR query instead of ANY. This reverse lookup will only work if the IP address owner has inserted a PTR record in the DNS. The PTR information is informal only and it may mostly be true, but sometimes not. If you don't get a PTR information about a specific computer from a NSLOOKUP query, you may want to try our whois service to find out the owner of this IP address.
Like the PTR, other records are also not mandatory: LOC, RP, TXT. They are not strictly required in the DNS and their content may be true or not.
You can't trust on the LOC to locate a host, because most hosts don't have this record defined.

If you prefer dig over nslookup, you may try our dig service.

This page is also available in German, French and Portuguese. Enjoy.
>>> If you would like to see this service in your or any other language, please send a translation.

PayPal DONATE If you like this service, please, consider to make a small donation to fund and continue this site. Thank you.

Link to www.kloth.net.

Recommended books about Networking.

You are coming from IP address **110.225.32.150** using port 51846.
A DNS reverse lookup on this IP address does not work.

You are talking to server www.kloth.net (78.46.75.45) on port 80 using the protocol HTTP/1.1
Current date and time (UTC) on the server is 2025-03-14 (Fri) 10:00:38. It is the 73rd day of tl

Start

KLOTH.NET | Services | Radio | Internet | Software | Support | Aircraft | Links...

www.kloth.net > services > nslookup

NSLOOKUP: look up and find IP addresses in the DNS

Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.

This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.
This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.

NSlookup

Domain: intellipaat.com ... the name of the machine to look up.

Server: localhost ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query: A (IPv4 address) Look it up

... here is the **nslookup** result for **intellipaat.com** from server localhost, querytype=A :

```
DNS server handling your query: localhost
DNS server's address:  127.0.0.1#53

Non-authoritative answer:
Name:  intellipaat.com
Address: 104.18.26.176
Name:  intellipaat.com
Address: 104.18.27.176
```

[Query 1 of max 100]

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page).
Basically, DNS maps domain names to IP addresses.
Although this web online service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver "localhost"/127.0.0.1.
To resolve an IP address by reverse lookup (get a computer's name if you only have its IP address), try to perform a PTR query instead of ANY. This reverse lookup will only work if the IP address owner has inserted a PTR record in the DNS. The PTR information is informal only and it may mostly be true, but sometimes not. If you don't get a PTR information about a specific computer from a NSLOOKUP query, you may want to try our whois service to find out the owner of this IP address.
Like the PTR, other records are also not mandatory: LOC, RP, TXT. They are not strictly required in the DNS and their content may be true or not.

NSLOOKUP: look up and find IP addresses in the DNS

Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.

This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.
This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.

NSlookup

Domain: intellipaat.com ... the name of the machine to look up.

Server: localhost ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query: A (IPv4 address) Look it up

... here is the **nslookup** result for **intellipaat.com** from server localhost, querytype=MX :

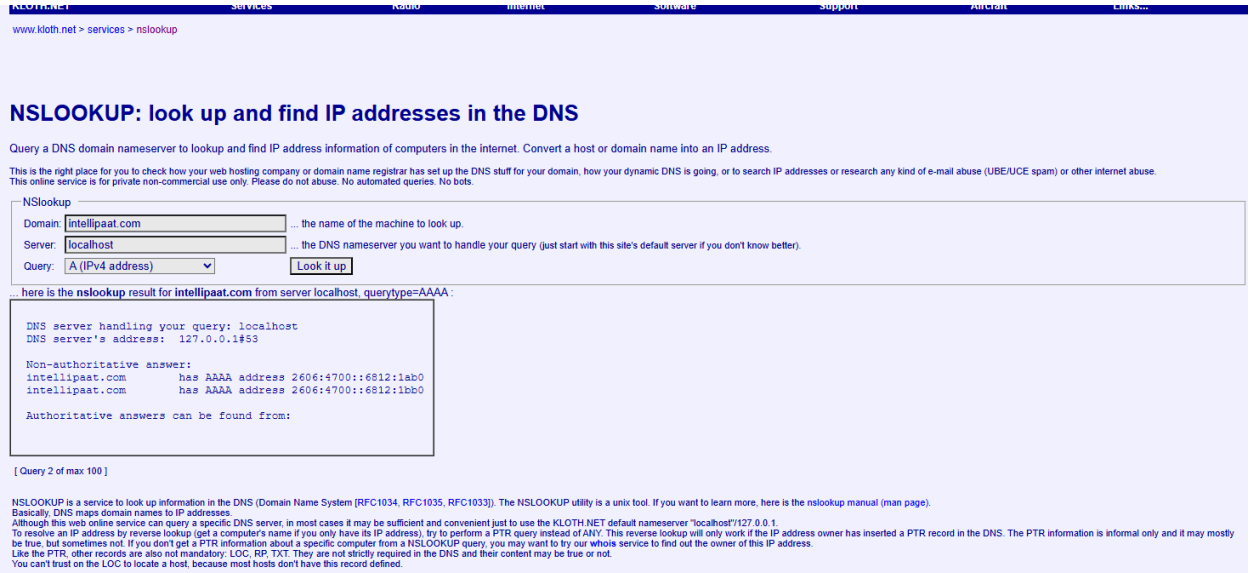
```
DNS server handling your query: localhost
DNS server's address:  127.0.0.1#53

Non-authoritative answer:
intellipaat.com        mail exchanger = 5 alt2.aspmx.l.google.com.
intellipaat.com        mail exchanger = 10 alt3.aspmx.l.google.com.
intellipaat.com        mail exchanger = 10 alt4.aspmx.l.google.com.
intellipaat.com        mail exchanger = 1 aspmx.l.google.com.
intellipaat.com        mail exchanger = 5 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
```

[Query 4 of max 100]

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page).
Basically, DNS maps domain names to IP addresses.
Although this web online service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver "localhost"/1

Microsoft Store

To resolve an IP address by reverse lookup (get a computer's name if you only have its IP address), try to perform a PTR query instead of ANY. This reverse lookup will only wor... ...mer has inserted a PTR record in the DNS. The PTR information is informal only and it may mostly



Detailed report and vulnerabilities with loopholes

TheHarvester has found **4 email IDs** and **27 hosts** during footprinting, it indicates that the target is leaking potentially sensitive information. Publicly exposed email addresses increase the risk of **phishing attacks, spam, and credential stuffing** and 27 hosts found indicate potential attack surfaces, misconfigured subdomains, and security vulnerabilities.

Recommendations for improving the security: Use Email Masking – Replace direct emails with contact forms or generic support emails, Enable Multi-Factor Authentication (MFA) – Protect exposed email accounts by enforcing MFA. Perform Subdomain Enumeration & Cleanup **–** Remove unused, misconfigured, or abandoned subdomains.

Using nslookup command line utility and online tool, we got the primary name server and IP address, DNS IP address, mail exchange domain, these findings indicate potential security risks. Primary name server can lead to DNS hijacking, zone transfer attacks, and cache poisoning. DNS IP address can lead to DDoS attacks, unauthorized access, and reconnaissance. MX record can allow attackers to target email servers for phishing, spoofing, and MITM attacks.

Recommendations for improving the security: Restrict Zone Transfers, Use Secure DNS Protocols, Harden Name Servers. Use Cloud-Based DNS Protection: Deploy services like Cloudflare, Akamai, or Quad9 to protect against DDoS and DNS tunneling attacks. Disable Unnecessary DNS Records, Deploy Web Application Firewall (WAF) and Regular Security Audits.