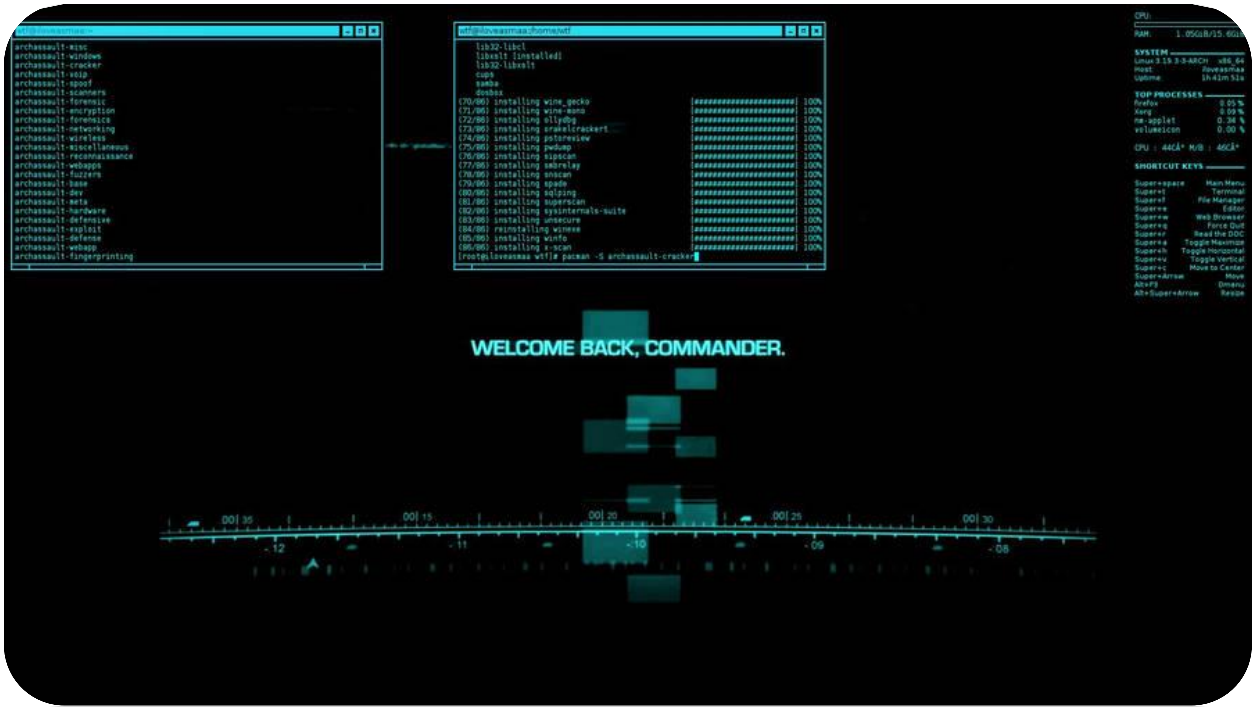
Advanced Footprinting and Reconnaissance Report



```
archassault-misc
archassault-windows
archassault-cracker
archassault-voip
archassault-spoof
archassault-scanners
archassault-forensic
archassault-encryption
archassault-forensics
archassault-networking
archassault-wireless
archassault-miscellaneous
archassault-reconnaissance
archassault-webapps
archassault-fuzzers
archassault-base
archassault-dev
archassault-meta
archassault-hardware
archassault-defensive
archassault-exploit
archassault-defense
archassault-webapp
archassault-fingerprinting
```

```
    lib32-libcl
    libxslt [installed]
    lib32-libxslt
    cups
    samba
    dosbox
(70/86) installing wine_gecko                 [######################] 100%
(71/86) installing wine-mono                  [######################] 100%
(72/86) installing ollydbg                    [######################] 100%
(73/86) installing orakelcrackert             [######################] 100%
(74/86) installing pstoreview                 [######################] 100%
(75/86) installing pwdump                     [######################] 100%
(76/86) installing sipscan                    [######################] 100%
(77/86) installing smbrelay                   [######################] 100%
(78/86) installing snscan                     [######################] 100%
(79/86) installing spade                      [######################] 100%
(80/86) installing sqlping                    [######################] 100%
(81/86) installing superscan                  [######################] 100%
(82/86) installing sysinternals-suite         [######################] 100%
(83/86) installing unsecure                   [######################] 100%
(84/86) reinstalling winexe                   [######################] 100%
(85/86) installing winfo                      [######################] 100%
(86/86) installing x-scan                     [######################] 100%
[root@iloveasmaa wtf]# pacman -S archassault-cracker
```

Author

Farwa Shaikh

www.linkedin.com/in/farwa-shaikh06/

https://github.com/farwa-shaikh

📜 Disclaimer

This reconnaissance report on the domain digiskills.pk has been prepared strictly for educational purposes and to demonstrate ethical security assessment techniques. All information was collected using legal Open Source Intelligence (OSINT) methods and controlled, non-intrusive active reconnaissance techniques that do not exploit, harm, or alter the target system in any way. Tools such as whois, nslookup, nmap, netcat, and Google Dorking were used within safe scanning parameters (e.g., -sn, -sS, -sV, -O) to minimize the risk of detection or disruption. No unauthorized access, penetration, or exploitation was performed. No data was modified, stolen, or damaged. All commands were executed in a controlled environment or simulated where applicable. Any interaction with the target was strictly passive or within safe bounds of active footprinting. I confirm that this activity was conducted with respect to all legal and ethical boundaries, and takes full responsibility for adhering to any applicable laws and policies.

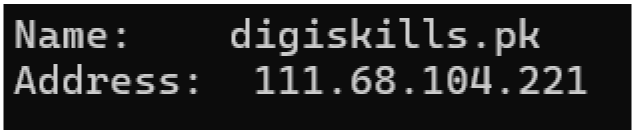
Task Objective:

Perform passive and active footprinting on a given target domain "https://digiskills.pk" to gather as much publicly available information as possible without triggering intrusion detection mechanisms. Document the process, tools, and findings while emphasizing legal and ethical boundaries.

Passive Reconnaissance (No direct interaction with the target)

Task Details:

Target: Use the domain or IP address (https://digiskills.pk). Do NOT attack or probe unauthorized live sites.



```
Name:    digiskills.pk
Address:  111.68.104.221
```

- **111.68.104.221 (Ip address of digiskills.pk)**

Step 1: Passive Reconnaissance

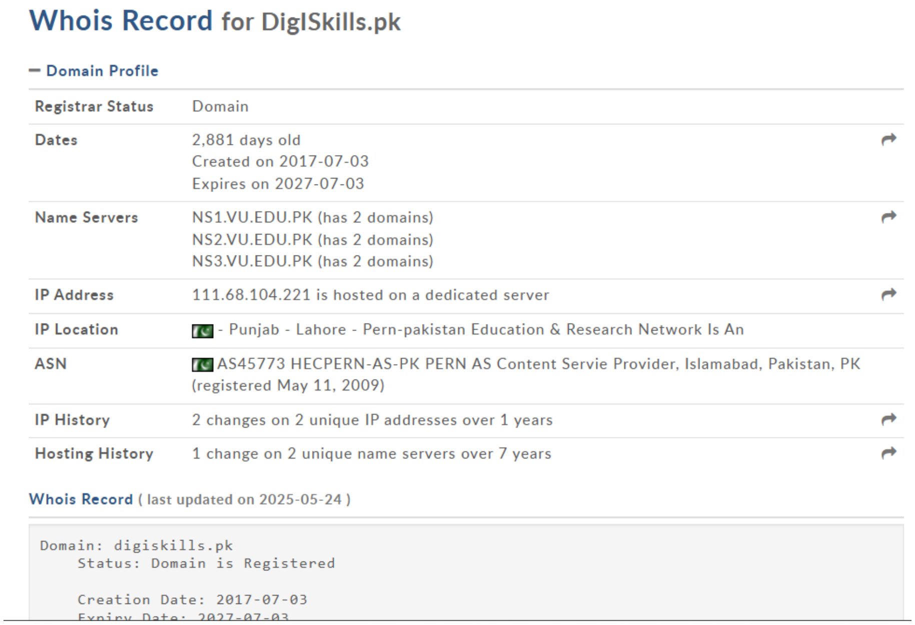
- Use OSINT techniques to gather information without direct interaction with the target.
- Identify the target's domain details, subdomains, IP ranges, and technologies used.

Tools/Techniques suggested:

- Whois Lookup (e.g., whois command, online Whois services)
- DNS Enumeration (e.g., dig, nslookup, online tools)
- Google Dorking for related info
- Search for data leaks or breaches associated with the domain
- Use Shodan or Censys to find exposed assets
- Gather email formats and employee info from LinkedIn or company website

Whois Lookup (e.g., **whois** command, online Whois services)

Find out **who owns the domain**, their **contact**, and **registration details**.



Whois Record for DigISkills.pk

— Domain Profile

Registrar Status	Domain
Dates	2,881 days old Created on 2017-07-03 Expires on 2027-07-03
Name Servers	NS1.VU.EDU.PK (has 2 domains) NS2.VU.EDU.PK (has 2 domains) NS3.VU.EDU.PK (has 2 domains)
IP Address	111.68.104.221 is hosted on a dedicated server
IP Location	🇵🇰 - Punjab - Lahore - Pern-pakistan Education & Research Network Is An
ASN	🇵🇰 AS45773 HECPERN-AS-PK PERN AS Content Servie Provider, Islamabad, Pakistan, PK (registered May 11, 2009)
IP History	2 changes on 2 unique IP addresses over 1 years
Hosting History	1 change on 2 unique name servers over 7 years

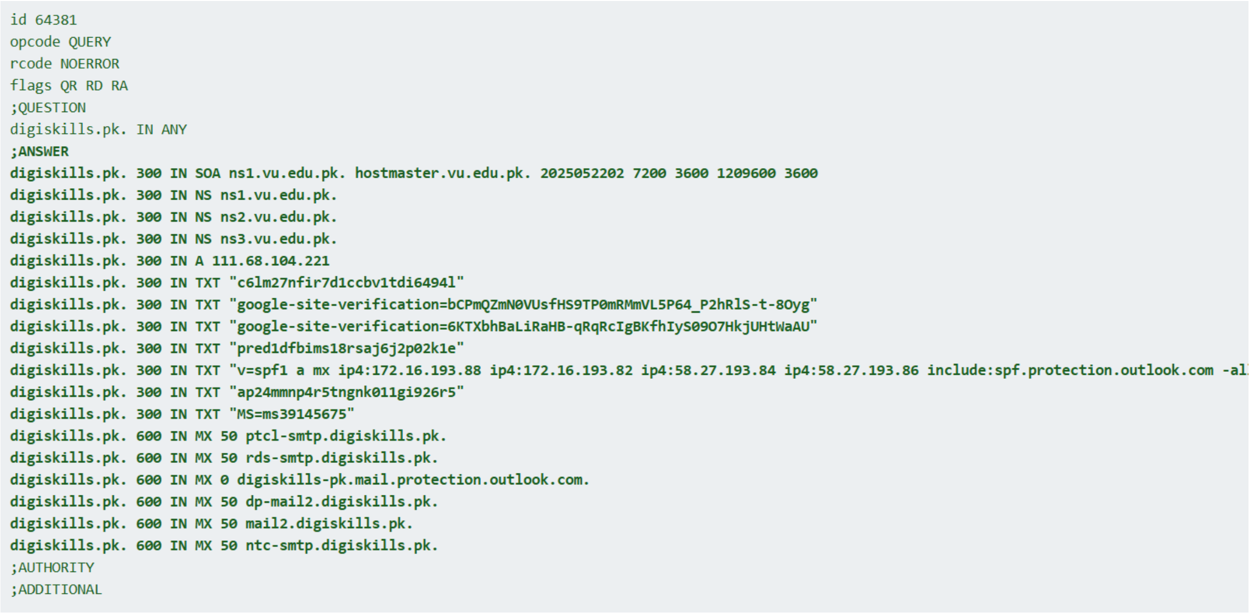
Whois Record (last updated on 2025-05-24)

```
Domain: digiskills.pk
    Status: Domain is Registered

    Creation Date: 2017-07-03
    Expiry Date: 2027-07-03
```

DNS Enumeration (e.g., dig, nslookup, online tools)

Discover **IP addresses**, **nameservers**, and possible **subdomains**.

Dig Results:



```
id 64381
opcode QUERY
rcode NOERROR
flags QR RD RA
;QUESTION
digiskills.pk. IN ANY
;ANSWER
digiskills.pk. 300 IN SOA ns1.vu.edu.pk. hostmaster.vu.edu.pk. 2025052202 7200 3600 1209600 3600
digiskills.pk. 300 IN NS ns1.vu.edu.pk.
digiskills.pk. 300 IN NS ns2.vu.edu.pk.
digiskills.pk. 300 IN NS ns3.vu.edu.pk.
digiskills.pk. 300 IN A 111.68.104.221
digiskills.pk. 300 IN TXT "c6lm27nfir7d1ccbv1tdi6494l"
digiskills.pk. 300 IN TXT "google-site-verification=bCPmQZmN0VUsfHS9TP0mRMmVL5P64_P2hRlS-t-8Oyg"
digiskills.pk. 300 IN TXT "google-site-verification=6KTXbhBaLiRaHB-qRqRcIgBKfhIyS09O7HkjUHtWaAU"
digiskills.pk. 300 IN TXT "pred1dfbims18rsaj6j2p02k1e"
digiskills.pk. 300 IN TXT "v=spf1 a mx ip4:172.16.193.88 ip4:172.16.193.82 ip4:58.27.193.84 ip4:58.27.193.86 include:spf.protection.outlook.com -al
digiskills.pk. 300 IN TXT "ap24mmnp4r5tngnk011gi926r5"
digiskills.pk. 300 IN TXT "MS=ms39145675"
digiskills.pk. 600 IN MX 50 ptcl-smtp.digiskills.pk.
digiskills.pk. 600 IN MX 50 rds-smtp.digiskills.pk.
digiskills.pk. 600 IN MX 0 digiskills-pk.mail.protection.outlook.com.
digiskills.pk. 600 IN MX 50 dp-mail2.digiskills.pk.
digiskills.pk. 600 IN MX 50 mail2.digiskills.pk.
digiskills.pk. 600 IN MX 50 ntc-smtp.digiskills.pk.
;AUTHORITY
;ADDITIONAL
```

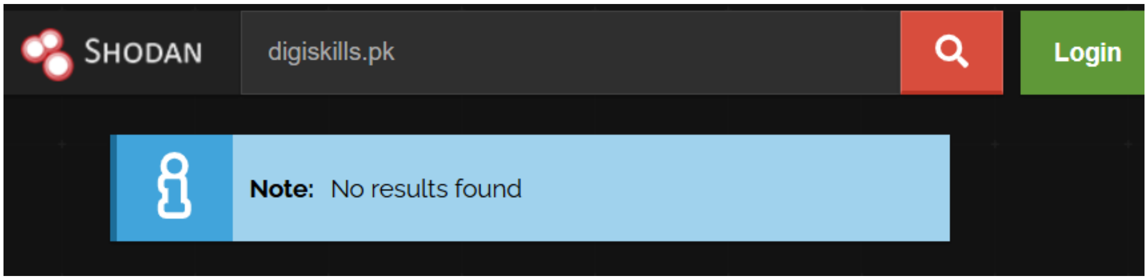
Google Dorking for related info

Use Google smartly to find **hidden or sensitive info** (PDFs, admin pages, leaks).

- site:digiskills.pk filetype:pdf
- site:digiskills.pk inurl:admin
- digiskills.pk" + "password"

Search for data leaks or breaches associated with the domain

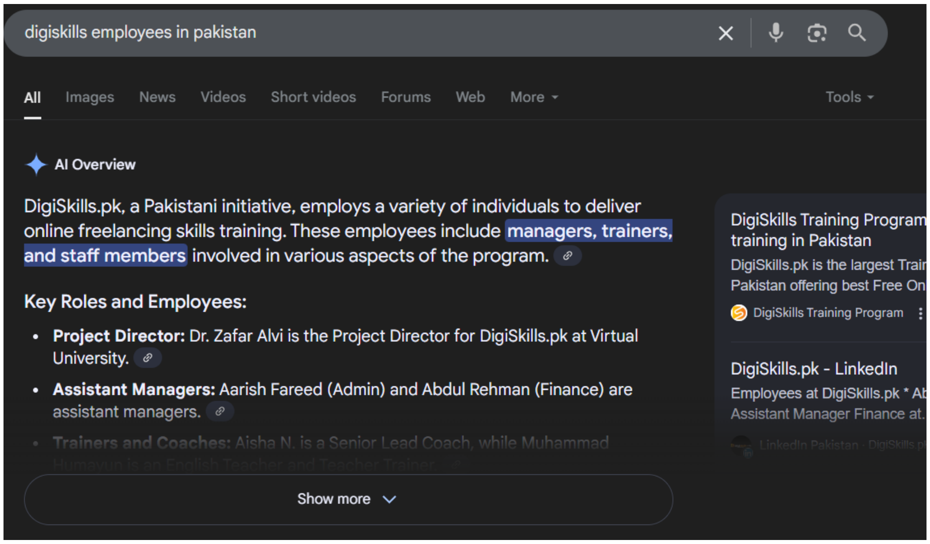
- **Use Shodan or Censys to find exposed assets**



Note: No results found

Gather email formats and employee info from LinkedIn or company website

- info@digiskills.pk
- tech_support@digiskills.pk



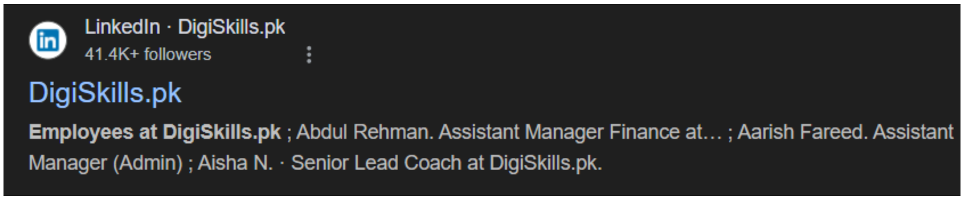
DigiSkills.pk, a Pakistani initiative, employs a variety of individuals to deliver online freelancing skills training. These employees include managers, trainers, and staff members involved in various aspects of the program.

Key Roles and Employees:

- **Project Director:** Dr. Zafar Alvi is the Project Director for DigiSkills.pk at Virtual University.
- **Assistant Managers:** Aarish Fareed (Admin) and Abdul Rehman (Finance) are assistant managers.
- **Trainers and Coaches:** Aisha N. is a Senior Lead Coach, while Muhammad Humayun is an English Teacher and Teacher Trainer.

DigiSkills Training Program training in Pakistan
DigiSkills.pk is the largest Trai
Pakistan offering best Free On
DigiSkills Training Program

DigiSkills.pk - LinkedIn
Employees at DigiSkills.pk * Ab
Assistant Manager Finance at.
LinkedIn Pakistan · DigiSkills.p



LinkedIn · DigiSkills.pk
41.4K+ followers

DigiSkills.pk

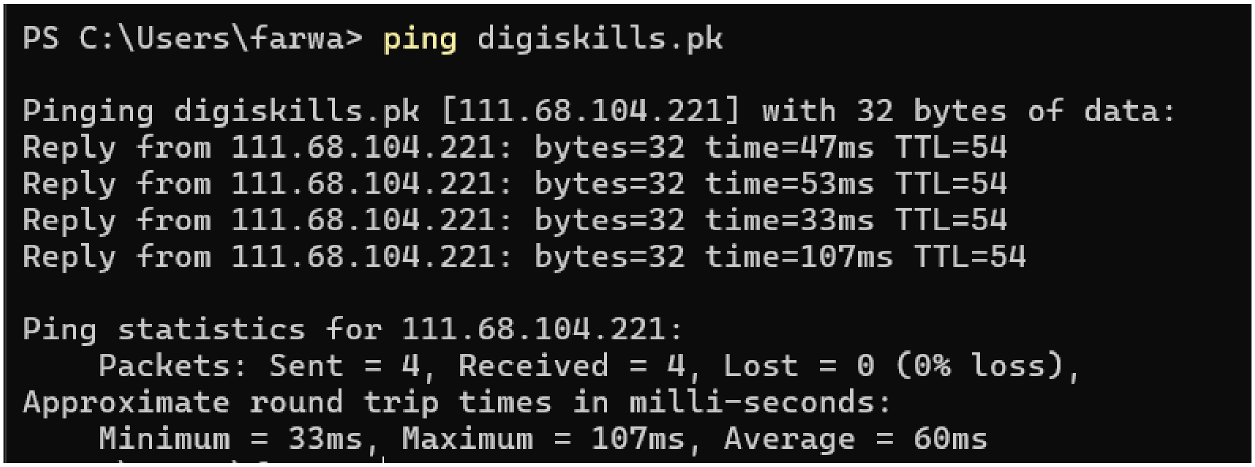
Employees at DigiSkills.pk ; Abdul Rehman. Assistant Manager Finance at… ; Aarish Fareed. Assistant Manager (Admin) ; Aisha N. · Senior Lead Coach at DigiSkills.pk.

Step 2: Active Reconnaissance

- Perform controlled interaction with the target to gather network and service details.
- Enumerate open ports, services, and versions without exploiting or causing harm.

Ping the Target

See if the target is **up and reachable**.



```
PS C:\Users\farwa> ping digiskills.pk

Pinging digiskills.pk [111.68.104.221] with 32 bytes of data:
Reply from 111.68.104.221: bytes=32 time=47ms TTL=54
Reply from 111.68.104.221: bytes=32 time=53ms TTL=54
Reply from 111.68.104.221: bytes=32 time=33ms TTL=54
Reply from 111.68.104.221: bytes=32 time=107ms TTL=54

Ping statistics for 111.68.104.221:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 107ms, Average = 60ms
```

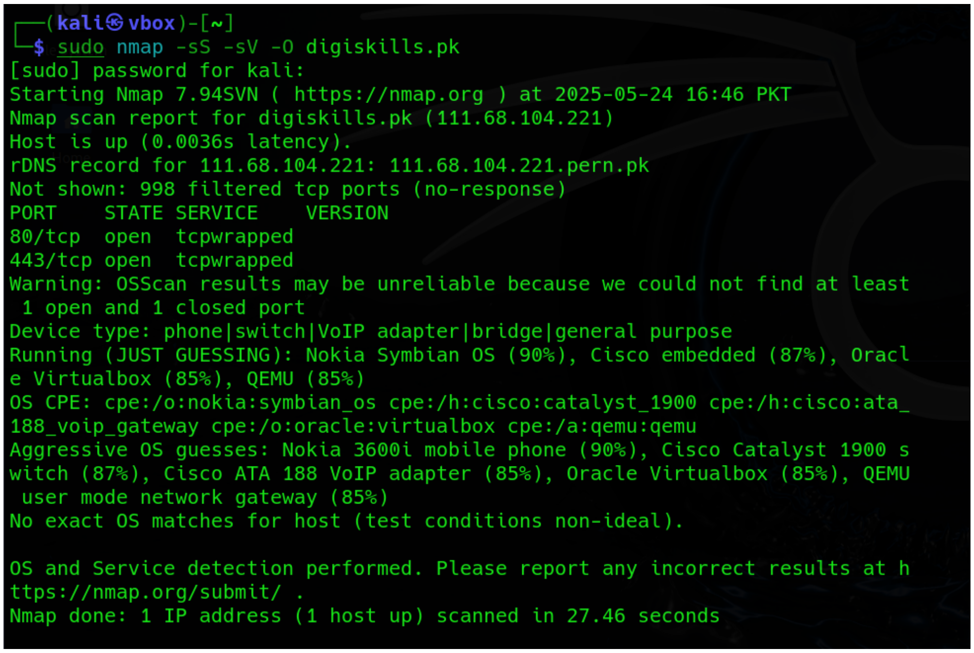
Tools suggested:

- Nmap with safe scanning options (e.g., SYN scan, version detection, OS fingerprinting)

Command: nmap -sS -sV -O digiskills.pk

- **sS: SYN scan (stealthy)**
- **sV: Version detection**
- **O: OS fingerprinting**

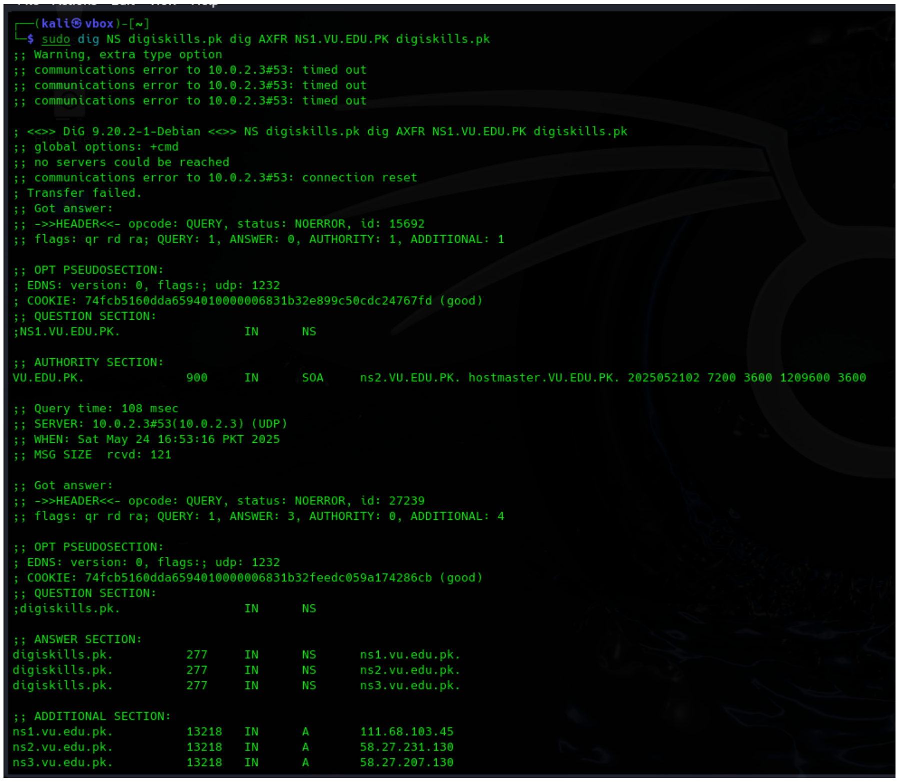
Result:



```
┌──(kali㉿vbox)-[~]
└─$ sudo nmap -sS -sV -O digiskills.pk
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-24 16:46 PKT
Nmap scan report for digiskills.pk (111.68.104.221)
Host is up (0.0036s latency).
rDNS record for 111.68.104.221: 111.68.104.221.pern.pk
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least
 1 open and 1 closed port
Device type: phone|switch|VoIP adapter|bridge|general purpose
Running (JUST GUESSING): Nokia Symbian OS (90%), Cisco embedded (87%), Oracl
e Virtualbox (85%), QEMU (85%)
OS CPE: cpe:/o:nokia:symbian_os cpe:/h:cisco:catalyst_1900 cpe:/h:cisco:ata_
188_voip_gateway cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Nokia 3600i mobile phone (90%), Cisco Catalyst 1900 s
witch (87%), Cisco ATA 188 VoIP adapter (85%), Oracle Virtualbox (85%), QEMU
 user mode network gateway (85%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.46 seconds
```

DNS Zone Transfer attempts

- See all the records for a domain (if misconfigured).
- **Command:** dig AXFR <nameserver> digiskills.pk – {AXFR (Asynchronous Full Transfer Zone) is a DNS zone transfer protocol.}



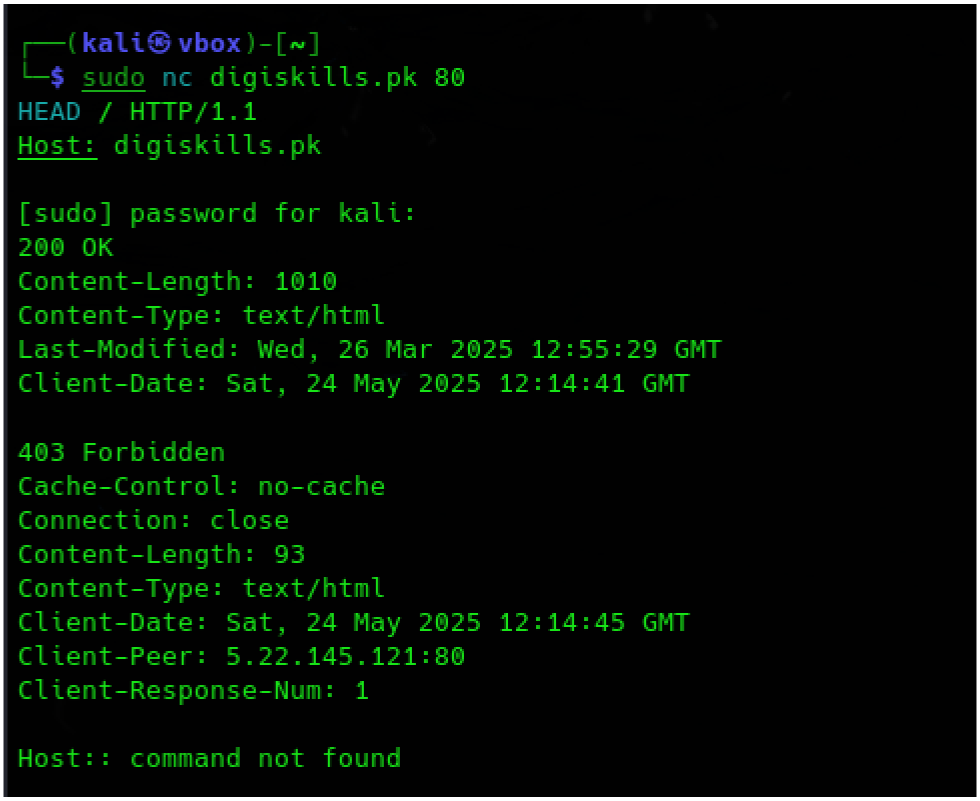
```
┌──(kali㉿vbox)-[~]
└─$ sudo dig NS digiskills.pk dig AXFR NS1.VU.EDU.PK digiskills.pk
;; Warning, extra type option
;; communications error to 10.0.2.3#53: timed out
;; communications error to 10.0.2.3#53: timed out
;; communications error to 10.0.2.3#53: timed out

; <<>> DiG 9.20.2-1-Debian <<>> NS digiskills.pk dig AXFR NS1.VU.EDU.PK digiskills.pk
;; global options: +cmd
;; no servers could be reached
;; communications error to 10.0.2.3#53: connection reset
; Transfer failed.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15692
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 74fcb5160dda6594010000006831b32e899c50cdc24767fd (good)
;; QUESTION SECTION:
;NS1.VU.EDU.PK.                 IN      NS

;; AUTHORITY SECTION:
VU.EDU.PK.              900     IN      SOA     ns2.VU.EDU.PK. hostmaster.VU.EDU.PK. 2025052102 7200 3600 1209600 3600

;; Query time: 108 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sat May 24 16:53:16 PKT 2025
;; MSG SIZE  rcvd: 121

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27239
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 74fcb5160dda6594010000006831b32feedc059a174286cb (good)
;; QUESTION SECTION:
;digiskills.pk.                 IN      NS

;; ANSWER SECTION:
digiskills.pk.          277     IN      NS      ns1.vu.edu.pk.
digiskills.pk.          277     IN      NS      ns2.vu.edu.pk.
digiskills.pk.          277     IN      NS      ns3.vu.edu.pk.

;; ADDITIONAL SECTION:
ns1.vu.edu.pk.          13218   IN      A       111.68.103.45
ns2.vu.edu.pk.          13218   IN      A       58.27.231.130
ns3.vu.edu.pk.          13218   IN      A       58.27.207.130
```

Banner grabbing using netcat or Telnet

- See what software/services are running by checking **response headers**.
- Connects to **digiskills.pk** on **port 80** (HTTP).
- Sends a **HEAD request**, which asks only for the **headers** (not the full web page).

Netcat (also called the "Swiss Army knife" of networking) is a simple, powerful tool used to:

- Connect to servers via TCP or UDP
- Manually send requests (like **HTTP,** FTP, SMTP)
- Grab service banners (to identify software and versions)



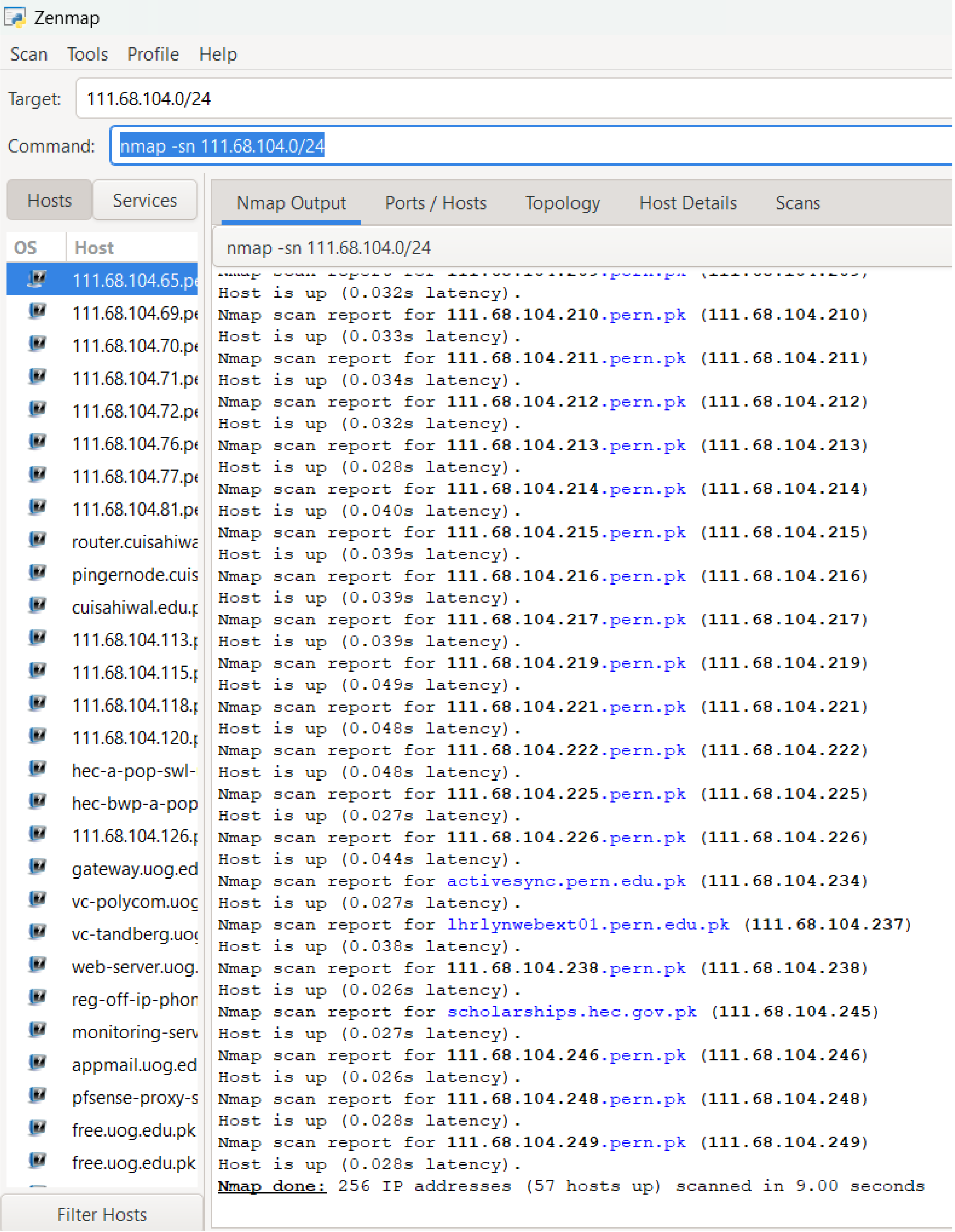
```
┌──(kali㉿vbox)-[~]
└─$ sudo nc digiskills.pk 80
HEAD / HTTP/1.1
Host: digiskills.pk

[sudo] password for kali:
200 OK
Content-Length: 1010
Content-Type: text/html
Last-Modified: Wed, 26 Mar 2025 12:55:29 GMT
Client-Date: Sat, 24 May 2025 12:14:41 GMT

403 Forbidden
Cache-Control: no-cache
Connection: close
Content-Length: 93
Content-Type: text/html
Client-Date: Sat, 24 May 2025 12:14:45 GMT
Client-Peer: 5.22.145.121:80
Client-Response-Num: 1

Host:: command not found
```

Ping sweep of IP range

🏠 Find out if there are **other live systems** on the same network.

- Command: nmap -sn 111.68.104.0/24
- -sn: Stands for "**ping scan**" (also called **host discovery**).

Results:



Target: 111.68.104.0/24

Command: nmap -sn 111.68.104.0/24

OS	Host
	111.68.104.65.pe
	111.68.104.69.pe
	111.68.104.70.pe
	111.68.104.71.pe
	111.68.104.72.pe
	111.68.104.76.pe
	111.68.104.77.pe
	111.68.104.81.pe
	router.cuisahiwa
	pingernode.cuis
	cuisahiwal.edu.p
	111.68.104.113.p
	111.68.104.115.p
	111.68.104.118.p
	111.68.104.120.p
	hec-a-pop-swl-
	hec-bwp-a-pop
	111.68.104.126.p
	gateway.uog.ed
	vc-polycom.uog
	vc-tandberg.uog
	web-server.uog.
	reg-off-ip-phon
	monitoring-serv
	appmail.uog.ed
	pfsense-proxy-s
	free.uog.edu.pk
	free.uog.edu.pk

nmap -sn 111.68.104.0/24

```
Nmap scan report for 111.68.104.209.pern.pk (111.68.104.209)
Host is up (0.032s latency).
Nmap scan report for 111.68.104.210.pern.pk (111.68.104.210)
Host is up (0.033s latency).
Nmap scan report for 111.68.104.211.pern.pk (111.68.104.211)
Host is up (0.034s latency).
Nmap scan report for 111.68.104.212.pern.pk (111.68.104.212)
Host is up (0.032s latency).
Nmap scan report for 111.68.104.213.pern.pk (111.68.104.213)
Host is up (0.028s latency).
Nmap scan report for 111.68.104.214.pern.pk (111.68.104.214)
Host is up (0.040s latency).
Nmap scan report for 111.68.104.215.pern.pk (111.68.104.215)
Host is up (0.039s latency).
Nmap scan report for 111.68.104.216.pern.pk (111.68.104.216)
Host is up (0.039s latency).
Nmap scan report for 111.68.104.217.pern.pk (111.68.104.217)
Host is up (0.039s latency).
Nmap scan report for 111.68.104.219.pern.pk (111.68.104.219)
Host is up (0.049s latency).
Nmap scan report for 111.68.104.221.pern.pk (111.68.104.221)
Host is up (0.048s latency).
Nmap scan report for 111.68.104.222.pern.pk (111.68.104.222)
Host is up (0.048s latency).
Nmap scan report for 111.68.104.225.pern.pk (111.68.104.225)
Host is up (0.027s latency).
Nmap scan report for 111.68.104.226.pern.pk (111.68.104.226)
Host is up (0.044s latency).
Nmap scan report for activesync.pern.edu.pk (111.68.104.234)
Host is up (0.027s latency).
Nmap scan report for lhrlynwebext01.pern.edu.pk (111.68.104.237)
Host is up (0.038s latency).
Nmap scan report for 111.68.104.238.pern.pk (111.68.104.238)
Host is up (0.026s latency).
Nmap scan report for scholarships.hec.gov.pk (111.68.104.245)
Host is up (0.027s latency).
Nmap scan report for 111.68.104.246.pern.pk (111.68.104.246)
Host is up (0.026s latency).
Nmap scan report for 111.68.104.248.pern.pk (111.68.104.248)
Host is up (0.028s latency).
Nmap scan report for 111.68.104.249.pern.pk (111.68.104.249)
Host is up (0.028s latency).
Nmap done: 256 IP addresses (57 hosts up) scanned in 9.00 seconds
```