

## ITA1443-ETHICAL HACKING LAB PROBLEMS

F. ABDUL RAHMAN 192124162

### EX-7: WHO.is

The screenshot shows the WHO.is website interface. The top navigation bar includes links for Premium Domains, Transfer, Features, Login, and Sign Up. The main header features the WHO.is logo and a search bar with the text "WHOIS Search, Domain Name, Website, and IP Tools". Below the search bar, a message indicates the user's IP address is 223.187.120.35. A blue banner below the header offers services: Looking to get a website?, Web Hosting, Website Builder, and SSL Certificates. The main content area is divided into three sections: "See Website Information" (Search the whois database, look up domain and IP owner information, and check out dozens of other statistics), "On Demand Domain Data" (Get all the data you need about a domain and everything associated with that domain anytime with a single search), and "Register Domain Names" (Find a domain with the best domain registrar on the web. Start your domain search at Name.com).

Below the main content area, there is a navigation bar with links for Transfers, Premium Domains, Web Hosting, Website Builder, Contact Us, FAQs, and Terms of Service. The second part of the screenshot shows the search results for "saveetha.com". The search bar contains "who.is/whois/saveetha.com". The results section is titled "saveetha.com" and "whois information". It includes tabs for Whois, DNS Records, and Diagnostics. A message indicates the cache expires in 16 minutes and 47 seconds, with a refresh button. The "Registrar Info" section lists the Name (PDR Ltd. d/b/a PublicDomainRegistry.com), Whois Server (whois.publicdomainregistry.com), Referral URL (www.publicdomainregistry.com), and Status (clientTransferProhibited https://icann.org/epp/clientTransferProhibited). The "Important Dates" section lists Expires On (2023-06-18), Registered On (2001-06-18), and Updated On (2022-05-27). The "Name Servers" section lists ns51.domaincontrol.com (97.74.105.26) and ns52.domaincontrol.com (173.201.73.26). The "Site Status" section lists Status (Active) and Server Type (Squarespace). The "Suggested Domains for saveetha.com" section lists save-etha.live for \$3.99. A promotional message from Name.com is also visible, offering a 15% discount on the first order using the promo code WHOIS.

Registrar Info	
Name	PDR Ltd. d/b/a PublicDomainRegistry.com
Whois Server	whois.publicdomainregistry.com
Referral URL	www.publicdomainregistry.com
Status	clientTransferProhibited https://icann.org/epp/clientTransferProhibited

Important Dates	
Expires On	2023-06-18
Registered On	2001-06-18
Updated On	2022-05-27

Name Servers	
ns51.domaincontrol.com	97.74.105.26
ns52.domaincontrol.com	173.201.73.26

Site Status	
Status	Active
Server Type	Squarespace

Suggested Domains for saveetha.com	
<input type="checkbox"/> save-etha.live	\$3.99

Sort by Popularity - Most

Watch Willow 1988 - Free

New Tab

Ethical-Hacking/Using Nm

New Tab

saveeetha.com DNS in

+

-

0

X

who.is

Search for domains or IP addresses...

Premium Domains

Transfer

Features

Login

Sign Up

saveeetha.com

DNS information

Whois

DNS Records

Diagnostics

DNS Records for saveeetha.com

Sort by Popularity - Most

Watch Willow 1988 - Free

New Tab

Ethical-Hacking/Using Nm

New Tab

saveeetha.com diagn

+

-

0

X

who.is

Search for domains or IP addresses...

Premium Domains

Transfer

Features

Login

Sign Up

saveeetha.com

diagnostic tools

Whois

DNS Records

Diagnostics

Ping

```
PING saveeetha.com (198.185.159.145) 56(84) bytes of data.
64 bytes from 198.185.159.145: icmp_seq=1 ttl=46 time=12.2 ms
64 bytes from 198.185.159.145: icmp_seq=2 ttl=46 time=8.28 ms
64 bytes from 198.185.159.145: icmp_seq=3 ttl=46 time=8.12 ms
64 bytes from 198.185.159.145: icmp_seq=4 ttl=46 time=8.14 ms
64 bytes from 198.185.159.145: icmp_seq=5 ttl=46 time=11.8 ms

--- saveeetha.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 8.127/9.708/12.234/1.902 ms
```

Traceroute

```
traceroute to saveeetha.com (198.185.159.144), 30 hops max, 60 byte packets
 1 10-10-0-0-14.ec2.internal (10.0.0.14) 1.316 ms 1.290 ms 1.301 ms
 2 216.182.231.46 (216.182.231.46) 25.820 ms 216.182.231.112 (216.182.231.112) 32.407 ms 216.182.226.58 (216.182.226.58) 25.755 ms
 3 100.66.9.228 (100.66.9.228) 70.729 ms 100.65.120.80 (100.65.120.80) 32.562 ms 100.66.9.4 (100.66.9.4) 27.690 ms
 4 100.66.11.216 (100.66.11.216) 12.826 ms 100.66.39.220 (100.66.39.220) 21.381 ms 100.66.11.76 (100.66.11.76) 15.299 ms
 5 241.0.4.208 (241.0.4.208) 1.899 ms 241.0.4.192 (241.0.4.192) 1.919 ms 241.0.4.205 (241.0.4.205) 1.874 ms
 6 241.0.4.195 (241.0.4.195) 1.919 ms 241.0.4.194 (241.0.4.194) 5.507 ms 240.0.40.27 (240.0.40.27) 5.315 ms
 7 240.0.40.17 (240.0.40.17) 1.255 ms 240.0.40.18 (240.0.40.18) 1.236 ms 240.0.40.19 (240.0.40.19) 1.237 ms
 8 242.0.170.17 (242.0.170.17) 2.169 ms 240.0.40.21 (240.0.40.21) 1.225 ms 240.0.40.28 (240.0.40.28) 3.016 ms
 9 52.93.28.177 (52.93.28.177) 1.743 ms 52.93.28.179 (52.93.28.179) 2.120 ms 242.0.171.1 (242.0.171.1) 1.644 ms
10 100.100.28.62 (100.100.28.62) 2.777 ms 52.93.28.193 (52.93.28.193) 30.496 ms 100.100.2.48 (100.100.2.48) 2.285 ms
```