

## **Footprinting and Reconnaissance**

Footprinting and reconnaissance are crucial phases in the process of hacking or attacking a target system. They involve gathering information about the target to understand its weaknesses and design an effective attack strategy. Here's a detailed explanation with examples:

**1. Footprinting :** Footprinting is the process of gathering as much information as possible about the target system or network before launching an attack. This information can include IP addresses, domain names, network infrastructure, employee details, and more. The goal is to identify the security posture of the target and find potential vulnerabilities.

❖ Examples of Footprinting Techniques:

- **Passive Footprinting:** This involves gathering information without directly interacting with the target. Examples include searching for information on search engines, social media platforms, and public databases.
- **Active Footprinting :** This involves directly interacting with the target to gather information. Examples include using tools like Nmap to scan for open ports, conducting network surveys, and using DNS interrogation techniques.

**2. Reconnaissance:** Reconnaissance is the next step after footprinting and involves using the gathered information to identify potential vulnerabilities and plan the attack strategy. It can be further divided into two types: network reconnaissance and application reconnaissance.

- **Network Reconnaissance:** This involves scanning the target network to identify live hosts, open ports, and services running on those ports. The goal is to identify potential entry points into the network.
- **Application Reconnaissance:** This involves gathering information about the applications running on the target network, such as web servers, email servers, and databases. The goal is to identify vulnerabilities in these applications that can be exploited.

## ❖ Examples of Reconnaissance Techniques:

- **Port Scanning:** Using tools like Nmap to scan for open ports on the target system, which can provide information about the services running on those ports.
- **Banner Grabbing:** Collecting information from banners or headers sent by the target system's services, which can reveal the software versions and sometimes even configuration details.
- **Vulnerability Scanning:** Using tools like Nessus or OpenVAS to scan for known vulnerabilities in the target system's software and services.

By performing thorough footprinting and reconnaissance, attackers can gather the information needed to launch a successful attack while defenders can use these techniques to identify and mitigate potential vulnerabilities. Information gathering in WHOIS website

## Domain information:

The screenshot displays the Whois website interface. At the top, a black banner promotes .COM domain registration for \$9.98. Below this, the navigation bar includes links for Domains, Hosting, Servers, Email, Security, Whois, and Deals. A search bar with the placeholder 'Enter Domain or IP' and a 'WHOIS' button is present. The main content area shows the 'vulnweb.com' domain information, updated 3 days ago. The 'Domain Information' section lists the domain name, registrar (EuroDNS S.A.), registration and expiration dates, update date, status (clientTransferProhibited), and name servers (ns1.eurodns.com, ns2.eurodns.com, ns3.eurodns.com, ns4.eurodns.com). The 'Registrant Contact' section shows the name 'Acunetix Acunetix' and the organization 'Acunetix Ltd'. To the right, a list of similar domains for sale is shown, including vulnwebonline.com, thevulnweb.com, vulnwebgroup.com, myvulnweb.com, vulnweb.net, and vulnwebonline.net, each with a 'Buy Now' button. A large red banner at the bottom right advertises '.space' domains for sale at \$1.88, down from \$29.88, with a 'BUY NOW' button. The browser's address bar shows 'whois.com/whois/vulnweb.com' and the Windows taskbar at the bottom displays the date and time as 13:38 on 20-05-2024.

Domain Information	
Domain:	vulnweb.com
Registrar:	EuroDNS S.A.
Registered On:	2010-06-14
Expires On:	2025-06-13
Updated On:	2023-05-26
Status:	clientTransferProhibited
Name Servers:	ns1.eurodns.com ns2.eurodns.com ns3.eurodns.com ns4.eurodns.com

Registrant Contact	
Name:	Acunetix Acunetix
Organization:	Acunetix Ltd


Interested in similar domains?	
vulnwebonline.com	Buy Now
thevulnweb.com	Buy Now
vulnwebgroup.com	Buy Now
myvulnweb.com	Buy Now
vulnweb.net	Buy Now
vulnwebonline.net	Buy Now

**.space**

~~\$29.88~~ **\$1.88**

**BUY NOW**

## Registrant contact:

 Registrant Contact	
Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	<b>administrator</b> @acunetix.com

## Administrative contact:

 Administrative Contact	
Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	<b>administrator</b> @acunetix.com

## Technical contact:



## Technical Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	<b>admin</b> istrator@acunetix.com

## Raw whois Data:

Domain Name: vulnweb.com

Registry Domain ID: D16000066-COM

Registrar WHOIS Server: whois.eurodns.com

Registrar URL: http://www.eurodns.com

Updated Date: 2023-05-26T10:04:20Z

Creation Date: 2010-06-14T00:00:00Z

Registrar Registration Expiration Date: 2025-06-13T00:00:00Z

Registrar: Eurodns S.A.

Registrar IANA ID: 1052

Registrar Abuse Contact Email: email@eurodns.com

Registrar Abuse Contact Phone: +352.27220150

Domain Status: client Transfer Prohibited

<http://www.icann.org/epp#clientTransferProhibited>

Registry Registrant ID:

Registrant Name: Acunetix Acunetix

Registrant Organization: Acunetix Ltd

Registrant Street: 3rd Floor,, J&C Building,, Road Town

Registrant City: Tortola

Registrant State/Province:

Registrant Postal Code: VG1110

Registrant Country: VG

Registrant Phone: +1.23456789

Registrant Fax:

Registrant Email: email@acunetix.com

Registry Admin ID:

Admin Name: Acunetix Acunetix

Admin Organization: Acunetix Ltd

Admin Street: 3rd Floor,, J&C Building,, Road Town

Admin City: Tortola

Admin State/Province:

Admin Postal Code: VG1110

Admin Country: VG

Admin Phone: +1.23456789

Admin Fax:

Admin Email: email@acunetix.com

Registry Tech ID:

Tech Name: Acunetix Acunetix

Tech Organization: Acunetix Ltd

Tech Street: 3rd Floor,, J&C Building,, Road Town

Tech City: Tortola

Tech State/Province:

Tech Postal Code: VG1110

Tech Country: VG

Tech Phone: +1.23456789

Tech Fax:

Tech Email: email@acunetix.com

Name Server: ns1.eurodns.com

Name Server: ns2.eurodns.com

Name Server: ns3.eurodns.com

Name Server: ns4.eurodns.com

DNSSEC: unsigned