

Footprinting and Reconnaissance

FOOT PRINTING:

Foot printing, in the context of cybersecurity, refers to the process of gathering information about a target system or network to identify vulnerabilities and gain access to it. There are several types of footprinting:

1. **Passive Footprinting:** This involves collecting information without directly interacting with the target system. It includes gathering data from public sources, such as websites, social media, and public records.
2. **Active Footprinting:** This type involves directly interacting with the target system to gather information. It can include techniques like port scanning, network scanning, and reconnaissance.
3. **Open Source Footprinting:** This involves using publicly available information from Sources like search engines, social media, and public databases to gather information about the target.
4. **DNS Footprinting:** This involves gathering information about the target's domain names, such as the domain name system (DNS) records, subdomains, and associated IP addresses.
5. **Social Engineering Footprinting:** This involves gathering information through social engineering techniques, such as phishing emails, to trick individuals into revealing sensitive information about the target.

RECONNAISSANCE:

Reconnaissance, also known as “recon,” is the process of gathering information about a target system or network to identify vulnerabilities and gather intelligence. It is a crucial phase in the process of a cyberattack. There are several types of reconnaissance:

1. **Network Reconnaissance:** This involves scanning the target network to gather information about active hosts, open ports, and services running on those ports. Techniques include ping sweeps, port scans, and service identification.
2. **Footprinting:** As mentioned earlier, this involves gathering information about the target from publicly available sources, such as websites, social media, and public records.
3. **OSINT (Open-Source Intelligence):** This involves using publicly available information to gather intelligence about the target, including information from social media, forums, and other online sources.
4. **Scanning:** This involves actively probing the target system or network to gather more detailed information, such as the operating system, running services, and potential vulnerabilities.
5. **Enumeration:** This involves actively querying the target system to gather information about users, shares, and other resources available on the system.
6. **Social Engineering:** This involves using psychological manipulation to trick individuals into revealing sensitive information about the target, such as passwords or system configurations.

Information gathering in WHOIS website

Domain information

The screenshot shows the Whois website interface. At the top, there's a banner for ".COM @ \$9.98" with a "BUY NOW" button. Below the banner, the navigation menu includes "Domains", "Hosting", "Servers", "Email", "Security", "Whois", and "Deals". A search bar with "Enter Domain or IP" and a "WHOIS" button is present. The main content area displays the domain "vulnweb.com" with a "Domain Information" section. To the right, there's a list of "Interested in similar domains?" with several domain names and "Buy Now" buttons. At the bottom right, there's a red banner for ".space" domains with a "Sale" tag and a "BUY NOW" button.

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 Sale	
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:	administrator@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:	administrator @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:	administrator @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: +1.23456789Admin

Fax:

Admin Email: email@acunetix.comRegistry

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: VG1110Tech

Country: VG

Tech Phone: +1.23456789Tech

Fax:

Tech Email: email@acunetix.comName

Server: ns1.eurodns.com Name Server:

ns2.eurodns.com Name Server:

ns3.eurodns.com Name Server:

ns4.eurodns.com DNSSEC: unsigned