Attack Phase

Footprinting

The objective ***of Footprinting:-***

- **Learn Security posture:** Analyze the target's security posture, find loopholes, and create an attack plan.
- **Identify focus area:** Using different tools and techniques, narrow down the range of IP addresses.
- **Find vulnerabilities:** Use the collected information to identify the target's security weaknesses.
- **Map the network:** Graphically represent the target's network and use it as a guide during the attack.

Collecting Network Information

- `Domain Name`
- `Internal domain Names`
- `Network blocks`
- `Rouge websites/Private websites`
- `Networking protocols`
- `IDSes running`
- `TCP and UDP services running`
- `Access control mechanisms and ACLs`
- `Active IP addresses`
- `VPN points`
- `Analog/digital Telephone numbers`
- `Authentication mechanisms`

Collecting Network Information

- User and group names
- System banners
- Routing tables
- SNMP information
- System architecture
- Remote system type
- System names
- Passwords

Collecting Organizational Information:

- Employee details
- Organization's website
- Company directory
- Location details
- Address and Phone numbers
- Commenting in GTML source code
- Security policies implemented
- Web server links relevant to the organization
- Background of the organization

- News articles/press releases

TOOLS:

WEB Mirroring

- httrack
- wget

Administrative Information

- whois (by icann)

DNS FOOTPRINTING

- DNSdumpster

Record	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

Start of Authority

Scanning Phase

Enumeration