Information Obtained in Footprinting

Organization information

- Employee details
- Telephone numbers
- Branch and location details
- Background of the organization
- Web technologies
- News articles, press releases, and related documents

Network information

- Domain and sub-domains
- Network blocks
- Network topology, trusted routers, and firewalls
- IP addresses of the reachable systems
- Whois records
- DNS records

System information

- Web server OS
- Location of web servers
- Publicly available email addresses
- Usernames and passwords

Lab: Passive Information Gathering using OSINT

- Download and install “**xmind**” application (https://xmind.app/)
- Using OSINT, gather information about “(Target) **telenor.com.pk**":-
  - Company Name
  - Key Services / Products
  - Scope of Services
  - Website
    - Fully Qualified Domain Name (FQDN)
    - Hosting Country / Company
    - Age
    - IP Address
    - Geo Location of Web Server (longitude/latitude)
    - Technologies
    - Load Balancer / Web Application Firewall (WAF), if any
  - Data centre Devices:-
    - Datacom (routers, switches)
    - Next Generation Firewall (NGFW) vendor
    - Network Time Protocol (NTP) Server
    - Apache Server
    - Web Application Firewall (WAF),if any
    - Load Balancer, if any

Lab: Passive Information Gathering using OSINT

- Using OSINT, gather information about “(Target) **Telenor Pakistan**":-
  - Content Delivery Network (if any)
  - Sub-domains
  - Domain Registrar
  - Shared hosting
  - Mail Servers
  - Name Servers (DNS)
  - Website Mirroring
  - Harvesting Email lists
  - Banner Grabbing / Determine Operating System
  - Acquisitions

Finding Sub-Domains

Finding sub-domains using “Subdomain Finder”

Finding sub-domains using assetfinder (linux)

Finding sub-domains using subfinder (Linux)
How to install: apt install subfinder

Finding sub-domains using crt.sh

Finding sub-domains using Amass

Finding sub domains using Google Dorks

Web site mirroring using Httrack / cyotek webcopy

Shodan.io

Banner Grabbing(Operating System) Using Censys

https://www.maltego.com/downloads/

exiftool image analyzer

Social Media profiler sherlock using kali Linux Apt install sherlock sherlock (username)

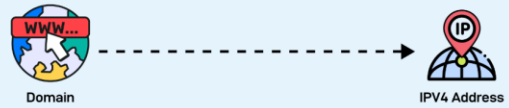
https://www.social-searcher.com/

Introduction
DNS Footprinting

DNS Record Types You Should Know

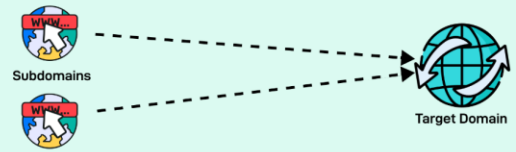
ByteByteGo

A (Address)



- Most commonly used DNS Record Type
- Used to map FQDN (Fully Qualified Domain Name) to an IPv4 address

CNAME



- Simplifies domain management by aliasing one domain name to another

TXT (Text)

domain	record	value
example	TXT	v=spf1 include:_spf.google.com ~all

- Allows DNS admins to add limited human & machine readable notes
- Use for verification records like SPF for email security

AAAA

- Maps domain name to an IPv6 address
- Used for websites that support IPv6

SRV

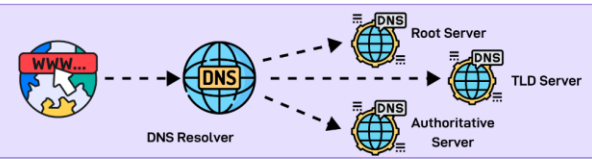
service	protocol	name	port
XMPP	TCP	example.com	5220

- SRV Record specifies a host & port for specific services such as VoIP
- Used in conjunction with A record

PTR

- Provides reverse DNS lookup, mapping an IP address to domain name

NS (Name Server)



- Specifies the authoritative DNS Servers for the domain
- Helps direct queries to correct DNS servers

MX (Mail)

- MX Record directs email traffic to the correct mail server
- Used in conjunction with A records

whois

- WHOIS databases is managed by Regional Internet Registries and is a listing of all registered domains and contain the personal information of domain owners.
- Managed by International Corporation for Assigned Names and Numbers (ICANN)
- Protects domain registrants by prohibiting the use of WHOIS listings for marketing or spam purposes
- Poses a security risk on personal information when not properly configured

whois

- **WHOIS query returns**:
  - Domain name details
  - Contact details of domain owner, email and phone number
  - Domain name servers
  - When a domain has been created
  - Expiry records
  - Records last updated

whois

- **Regional Internet Registries (RIRs)**:
  - AFRINIC (African Network Information Center)
  - LACNIC (Latin American and Caribbean Network Information Center)
  - RIPE (Reseaux IP Europeens Network Coordination Centre)
  - APNIC (Asia Pacific Network Information Center)
  - ARIN (American Registry for Internet Numbers)

DNS Footprinting

Extracting DNS Information

- Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks.
- DNS records provide important information about location and type of servers.
- Know about the network blocks those IP addresses belong to and other servers that may be in those network blocks

DNS + Resource + Records

DNS Footprinting

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
SDA	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

DNS Footprinting Using Dnsdumpster