TECHNOLOGY REDEFINE

Showing posts with label **DNS Enumeration & Interrogation.**
Show all posts

Sunday, September 17, 2017

FOOTPRINTING

Footprinting (Also Known As Reconnaissance) Is The Technique Used For Gathering Information About Computer Systems And The Entities They Belong To. To Get This Information, A Hacker Might Use Various Tools And Technologies. This Information Is Very Useful To A Hacker Who Is Trying To Crack A Whole System.

Footprinting Generally Refers To One Of The Pre-Attack Phases; Tasks Performed Prior To Doing The Actual Attack.

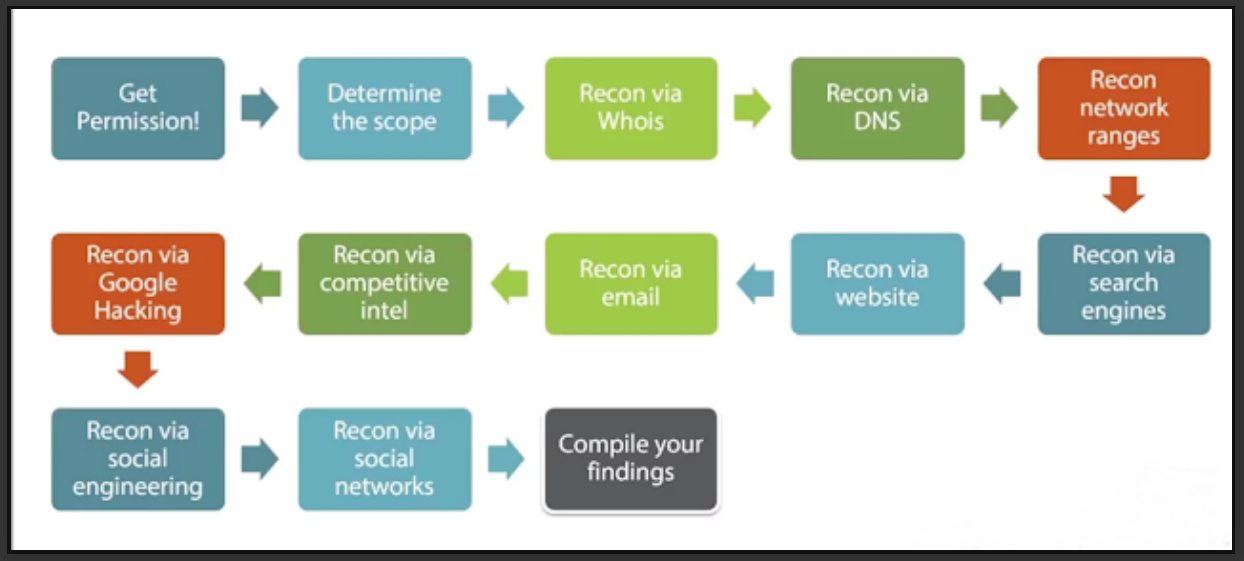
FOOTPRINTING STEPS

1. Getting Authorization
2. Defining the Scope of the Assessment

LABEL

- Cracking Hashes
- CVE-2018-0802
- DNS Enumeration & Interrogation
- Dump Hashes
- Dumpster-Diving
- Enumeration
- Evasion Techniques
- Finding Open Ports
- Firewall Evasion Countermeasures
- Footprinting Tools and Techniques
- Information Gathering
- Installing And Removing Application
- Installing VirtualBox Guest Addition
- Introduction To Linux
- Least privilege
- Linux Basic Commands
- MAC Spoofing

3. Finding Publicly Available Information
4. Visiting Physical Location
5. DNS Interrogation



1. Getting Authorization

- Get Proper Authorization In Writing From Right Person
- Decide Your Activities
- Get-Out-Of-Jail-Free Card

2. Defining the Scope of the Assessment

- Entire Organization
- Certain Locations

- Network Access Control
- Nmap Cheatsheet
- Nmap Scanning
- NTLM Hashes
- Password Hacking
- Password Hacking Countermeasures
- Password Sniffing
- payload generator
- post exploitation
- Reconnaissance
- Remote Access
- Reverse Proxy Server
- Risk Assessment
- Router Attacks
- Scanning
- Scanning Types
- Social Engineering
- Surveillance
- Virtual Ports
- Zone Transfer

- Business Partner Connections
- The Clients Disaster Recovery Sites

3. Finding Publicly Available Information

Network Information :
Domain Names, Internal Domain, IP Addresses, Unmonitored/Private Websites, TCP/UDP Services, IDS/Acess Controls, VPN Info, Phone Numbers/VOIP.

Operating System Information :
User & Groupnames/Info, Banner Grabbing, Routing Tables, SNMP, System Architecture, Remote System, System Names.

Organization Information :
Organization Website, Company Directory, Employee Details, Location Details, Address/Phone Numbers, Comments In HTML Source Code, Security Policy Deployed, Web Server Links, Background Of Organization, News/Press Releases.

Sources:

• Whois :

Domain Name
Registered Email
Owner Of Domain.

```
IP Address Range
Domain Expiration

• ICANN :

IP Address Blocks
Policy
Registries
Organizations

• Shodan :

Server Info
Running Services
SSL Certificate

• Wikipedia :

Date Of Birth, Family Info,
Location occupation, Salary,
Experience, Expertise
Job Status

• Events :

Social Engineering
Eavesdropping
Surveillance
```

```
• Wayback Machine :

History
Infrastructure
Emails, Phone Numbers

• People Search :

Phone Numbers, Emails, Location
Pipl, Spokeo, Google Groups

• Job Sites :

Running Server, Software, IDS
IPS, Database
Monster, Indeed, Careerbuilder,
Dice,  Glassdoor, Linkedin

• Social Sites :

LinkedIn, Facebook, Google Plus
Twitter
Employment, Education, Contact,
Interest, DOB, Friends, Likes,
Travels, Location, Family

• Search Engine :
```

```
Google, Yahoo, Bing,
Zabasearch, yandex

• Website :

Links
Source Code Comments

• Netcraft  : Website Report

• Censys : Certificate Analysis

• Remote Access : WebConnect
                  VPNs

• SEC Reports :

Financial Statement

• Vuln Research : nvd.nist.gov

• Quora
```

4. Visiting Physical Location

```
• Dumpster-Diving :
```

Dumpster Diving Is A Technique Used To Retrieve Information That Could Be Used To Carry Out An Attack On A Computer Network.
Dumpster Diving Isn't Limited To Searching Through The Trash For Obvious Treasures Like Access Codes Or Passwords Written Down On Sticky Notes. Seemingly Innocent Information Like A Phone List, Calendar, Or Organizational Chart Can Be Used To Assist An Attacker Using Social Engineering Techniques To Gain Access To The Network.

To Prevent Dumpster Divers From Learning Anything Valuable From Your Trash, Experts Recommend That Your Company Establish A Disposal Policy Where All Paper, Including Print-Outs, Is Shredded In A Cross-Cut Shredder Before Being Recycled, All Storage Media Is Erased, And All Staff Is Educated About The Danger Of Untracked Trash.

- Surveillance :

Hacker Do Surveillance In Order To Gain More Information About A Target It Can Be Done By Observation Of Target, Installing Hidden Cameras And Recording, Monitoring Every Action, Or Wiretapping Phone Calls.

- Social Engineering :

Social Engineering Is The Art Of Manipulating People So They Give Up Confidential Information. A Hacker Tricks You Into

Giving Them Your Passwords Or Bank Information, Or Access Your Computer To Secretly Install Malicious Software–That Will Give Them Access To Your Passwords And Bank Information As Well As Giving Them Control Over Your Computer.

Hackers Use Social Engineering Tactics Because It Is Usually Easier To Exploit Your Natural Inclination To Trust Than It Is To Discover Ways To Hack Your Software. For Example, It Is Much Easier To Fool Someone Into Giving You Their Password Than It Is For You To Try Hacking Their Password (Unless The Password Is Really Weak).

Security Is All About Knowing Who And What To Trust. Knowing When, And When Not To, To Take A Person At Their Word; When To Trust That The Person You Are Communicating With Is Indeed The Person You Think You Are Communicating With; When To Trust That A Website Is Or Isn’T Legitimate; When To Trust That The Person On The Phone Is Or Isn’T Legitimate; When Providing Your Information Is Or Isn’T A Good Idea.

Ask Any Security Professional And They Will Tell You That The Weakest Link In The Security Chain Is The Human Who Accepts A Person Or Scenario At Face Value. It Doesn’t Matter How Many Locks And Deadbolts Are On Your Doors And Windows, Or If Have Guard Dogs, Alarm Systems, Floodlights, Fences With Barbed Wire, And Armed Security Personnel; If You Trust The Person At The Gate Who Says He Is The Pizza Delivery Guy And You Let Him In Without First Checking To See If He Is Legitimate You Are

Completely Exposed To Whatever Risk He Represents.

Social Engineering Attacks:

• Telling That Your Card Is Blocked Asking For Banking Info To Unlock Your Card (Don't Be A Victim)
• Email From A Friend Asking For Password (Call Him)
• Malicious Link (Do Not Click On Suspecious Links)
• Malicious Download (Only Download From Official Website)
• Urgently Ask For Your Help (Verify Identity, Investigate)
• Asks You To Donate For Charity (Do Reserch)
• The Message May Explain There Is A Problem (Fake Software Update)
• The Message May Notify You That You’Re A ’Winner’ (You Can't Be A Winner Without Doing Anything)

Social Engineering Countermeasures :

• Remove Publically Available Sensitive Information.
• Restrict Zone Transfers To Only Authorized Servers.
• Implement Cryptographic Transaction Signatures (TSIGS).
• Configure External Name Servers To Provide Information Only About Systems Directly Connected To The Internet.

5. DNS Enumeration & Interrogation

DNS Enumeration Is The Process Of Locating All The DNS Servers

And Their Corresponding Records For An Organization. A Company May Have Both Internal And External DNS Servers That Can Yield Information Such As Usernames, Computer Names, And IP Addresses Of Potential Target Systems.

- DNSRecon (DNS Lookup, Reverse Lookup Range)
- Fierce (Zone Transfer, Subdomain Bruteforce, Subnet)
- ReconDog (Cloudfare, Honeypot, Links, Trace)
- RedHawk (CMS, IP Lookup, Banner, Subdomain)

Footprinting Countermeasures:

- Deploy Access Control List On Network Appliances
- Follow Least Privilege Model When Defining Access
- Disable Insecure & Unused Ports, Protocols
- Enforce Security Policies
- Keep Signatures Up To Date (IPS/AV)
- Keep Interanl DNS & External DNS Separate
- Disable Unnecessary Services
- Use VPN For Connecting Remotely
- Educate Employees To Be Aware Of The Info They Share On Social Sites
- Prevent Search Engines From Caching Web Pages
- Use Anonymous Registration Services
- Configure Web Server To Avoid Information Leakage
- Remove Sensitive Information From The Internet
- Keep Software Up To Date
- Disable Directory Listings

- Use TCP/IP & IPsec Filters
- Configure IIS Against Banner Grabbing
- Private Registration

FOOTPRINTING TOOLS:

- Samspade
- FOCA
- Theharvester
- SuperScan
- Recon-ng
- HTTrack
- Web Crawler
- SiteDigger
- Maltego
- Nikto

SOME USEFUL SITES:

Ultratools
View Cached
Link Extractor
Blasze (IP Logger)
Cloud piercer (Check Exposed IPs)
SEMRush (SEO Tool)
Email Header Analyser
Mxtoolbox
Pentest-tools

What Should Be on the Report

Data found via search engines

- Employee details:
- Login pages:
- Intranet portals
- Technology platforms
- Other

Data found via website

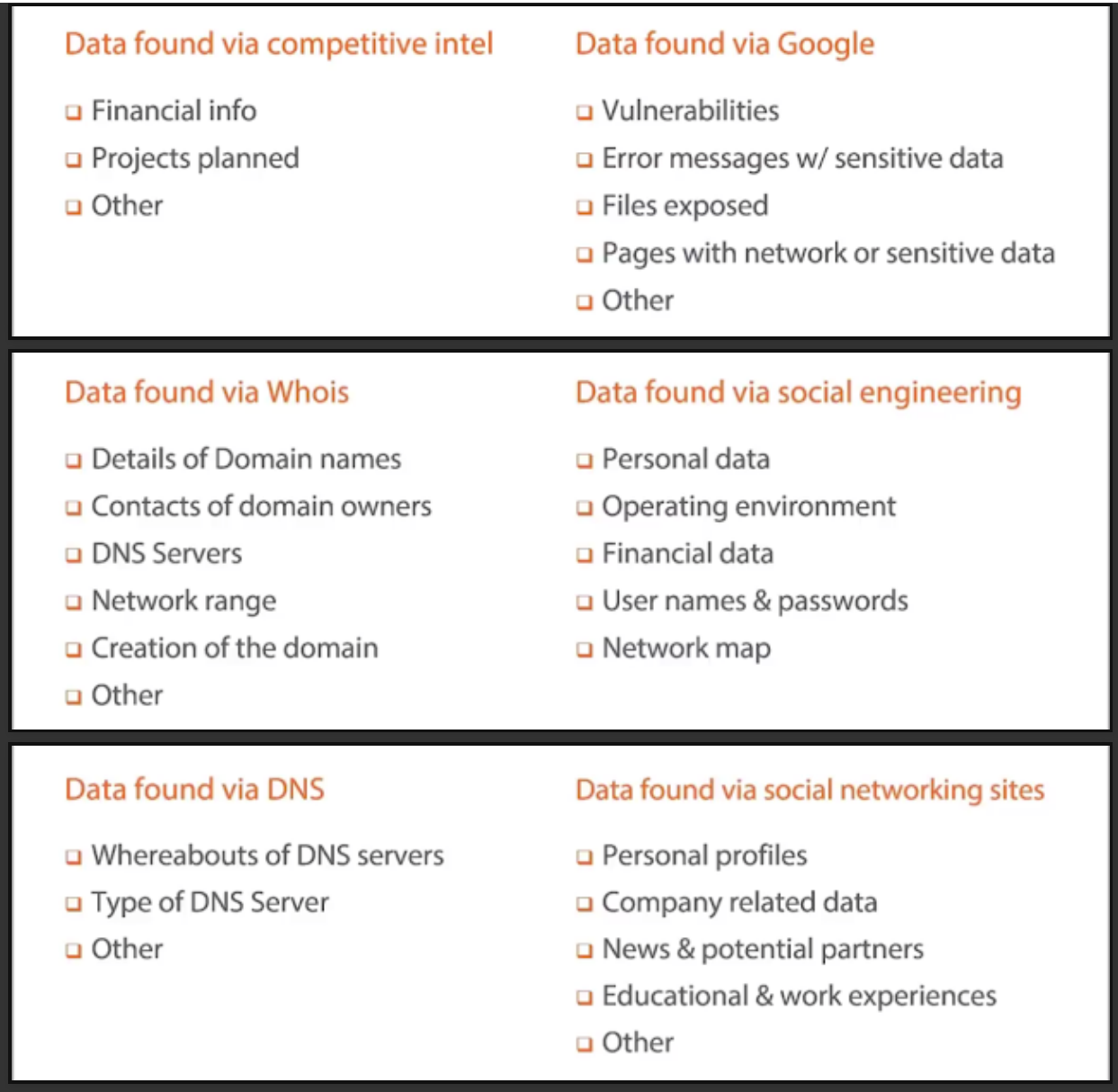
- Operating environments
- File system structure
- Scripting platforms
- Contact info
- CMS info
- Other

Data found via people search

- Contact info
- Birthdates
- Emails
- Photos
- Other

Data found via email

- IP addresses
- GPS location
- Authentication systems
- Other



By Himanshu - September 17, 2017

Ph?n ?ng: funny (0) interesting (0) cool (0)

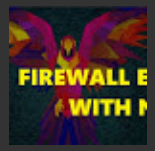
1 comment

Labels: DNS Enumeration & Interrogation, Dumpster-Diving, Footprinting Tools and Techniques, Information Gathering, Reconnaissance, Social Engineering, Surveillance

Home Older Posts

Subscribe to: Posts (Atom)

Popular Posts



IDS, IPS AND FIREWALL EVASION USING NMAP

NIDS – Network Intrusion Detection System • It Uses a network tap, span port, or hub to collect packets on the network • Attempts t...

INCIDENT RESPONSE PLAN

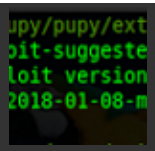
An incident response plan (IRP) is a set of written instructions for detecting, responding to and limiting the effects of an information...

INSTALLING PRESISTENCE BACKDOOR IN WINDOWS

USING METASPLOIT windows/local/s4u_persistence windows/local/vss_persistence windows/local/registry_persistence windows/manage...

NMAP CHEAT SHEET

Target Specification 192. 168. 100. 1-50 IP Range 192. 168. 100. 1/24 CIDR Spec. -iL Filename IP Addr File -iR...



WINDOWS-EXPLOIT-SUGGESTER

./windows-exploit-suggester.py --update This will download latest ms bulletin xls file pip install xlrd --upgrade to download xl...

PUPY (RAT, POST EXPLOITATION TOOL)

Installing pupy git clone https://github.com/n1nj4sec/pupy.git pupy cd pupy git submodule init git submodule update pip install -r pu...

Exploit Office 2016 using CVE-2018-0802

If you don't have Empire download from here Just run ./setup/install.sh to install Also Download Exploit for CVE-2018-0802   Cr...

Comment