BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

SSZG575: Footprinting and Scanning
Session No: 06

Agenda

- Footprinting
  - What Is Footprinting?
  - Why Is Footprinting Necessary?
  - Internet Footprinting
    - Determine the Scope of Your Activities
    - Get Proper Authorization
    - Publicly Available Information
    - WHOIS & DNS Enumeration
    - DNS Interrogation
    - Network Reconnaissance

- Scanning
  - Determining If the System Is Alive
  - Host Discovery: ARP, ICMP, TCP/UDP
  - Determining Which Services Are Running or Listening
  - Scan Types
  - Identifying TCP and UDP Services Running
  - Detecting the Operating System
  - Making Guesses from Available Ports
  - Active & Passive Stack Fingerprinting
  - Processing and Storing Scan Data
  - Managing Scan Data with Metasploit

Footprinting

What is Footprinting?

- Footprinting is the blue printing of the security profile of an organization undertaken in a structured manner.
- Footprinting is one of the 3 pre-attack phases. The other two are scanning and enumeration.
- Footprinting results in a unique organization profile with respect to networks (internet, Intranet, Extranet, Wireless) and systems involved.
- Using a combination of tools and techniques, attackers can take an unknown entity and reduce it to a specific range of domain names, networks, subnets, routers, IP addresses and other details about its security posture.
- An attacker will spend 90% of his time in profiling an organization and 10% in launching the attack.

Web Tools for Footprinting

Tool	Function
Google groups (*http://groups.google.com*)	Search for e-mail addresses in postings in technical or nontechnical newsgroups
Whois (*www.arin.net* or *www.whois.net*)	Gather IP and domain information
SamSpade (*www.samspade.org*)	Gather IP and domain information; versions available for UNIX and Windows OSs
Google search engine (*www.google.com*)	Search for Web sites and company data
Namedroppers (*www.namedroppers.com*)	Run a domain name search; more than 30 million domain names updated daily
White Pages (*www.whitepages.com*)	Conduct reverse phone number lookups and retrieve address information
Metis (*www.severus.org/sacha/metis*)	Gather competitive intelligence from Web sites
Dig (command available on all *NIX-based systems; can be downloaded from *http://pigtail.net/LRP/dig/* for Microsoft platforms)	Perform DNS zone transfers; replaces the Nslookup command
Host (command available on all *NIX-based systems; Hostname can be downloaded from *http://sysinternals.com/ntw2k/source/misc.shtml* for Windows platforms)	Obtain host IP and domain information; can also be used to initiate DNS zone transfers
Netcat (command available on all *NIX-based systems; can be downloaded from *http://atstake.com/research/tools* for Windows platforms)	Read and write data to ports over a network
Wget (command available on all *NIX-based systems; can be downloaded from *http://gnu.org/software/wget/wget.html* for Microsoft platforms)	Retrieve HTTP, HTTPS, and FTP files over the Internet
Paros (*www.parosproxy.org*)	Capture Web server information and possible vulnerabilities in a Web site's pages that could allow exploits such as SQL injection and buffer overflows

Determine the scope of activities

- Are you going to footprint the entire organization, or limit your activities to certain subsidiaries or locations?
- What about business partner connections (extranets), or disaster-recovery sites?
- Are there other relationships or considerations?
- Are you going to exploit the weaknesses in whatever forms they manifest themselves?
- What are the potential potential crack in your system?

Get proper authorization

innovate achieve lead

- Do you have authorization to proceed with your agreed list of activities?
- Is the authorization from the right person(s)?
- Is it in writing? Are the target IP addresses the right ones?
- Has senior leadership of the organization been informed of this?

Information gathering methodology

- Discover initial information
- Locate the network range
- Ascertain active machine
- Discover open ports / access points
- Detect operating systems
- Uncover services on ports
- Map the network

Discovering initial information

- Commonly include following:
  - Domain name lookup
  - Locations
  - Contacts (telephone, mails etc)
- Main information sources are:
  - Open source
  - Whois
  - Nslookup
- Hacking tools
  - Sam spade

Publicly available information

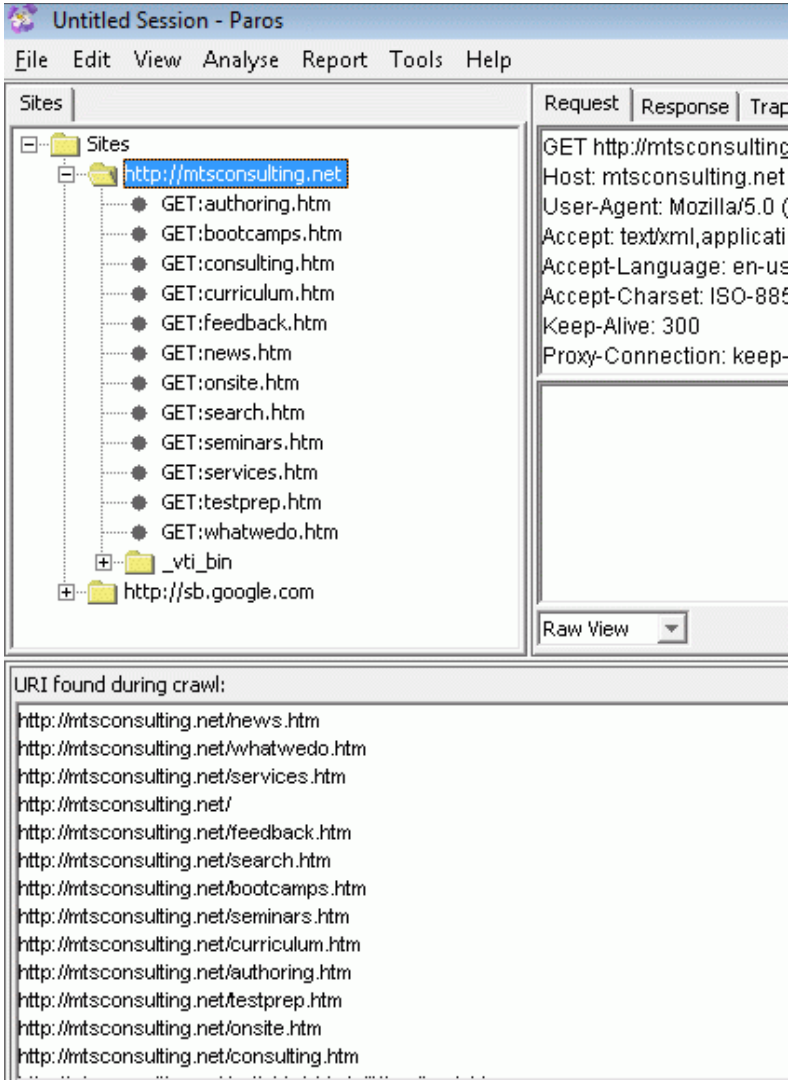
- Huge amount of information is readily available about an entity on internet. Some places are:
  - Company web pages: Review public website source code for comments in source code
  - Related organizations
  - Location details
  - Employee information
  - Current events
  - Privacy and security polices, and technical details indicating type of security mechanism in place
  - Archived information
  - Search engines and data relationships
  - Other information of interest

Company website

- Websites may have name, phone numbers, emails of key persons.
- Comments in HTML source code may contain important details.
- Mirror website for off-line code review.
- Good trusted website mirroring tools:
  - Wget (gnu.org/software/wget/wget.html) for UNIX/Linux
  - Teleport Pro (tenmax.com) for Windows
- Use brute-force techniques to enumerate “hidden” files and directories on a website:
  - Use OWASP’s DirBuster to do this automatically
- Investigate other sites beyond the main “http://www” and “https://www” sites as well. Sites like www1, www2, web, web1, test, test1 etc. are all great places for footprinting.

Paros: Tool to Analyze Website

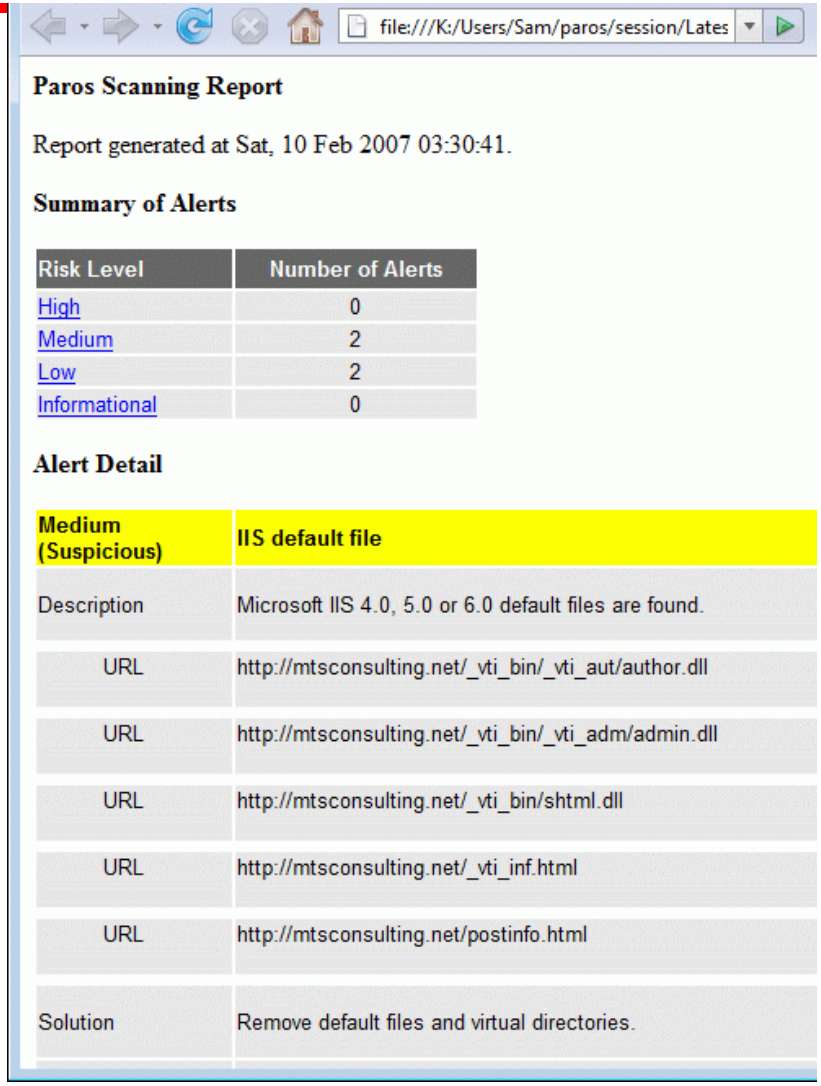
- Powerful tool for UNIX and Windows
- Can be downloaded from *www.parosproxy.org*
- Requires having Java J2SE installed
- Has features to
  - Analyze
  - Spider
- Finds all the pages in a site



Paros: Tool to Analyze Website

innovate achieve lead

- Identifies security risks in the site
- Don’t scan sites without permission



file:///K:/Users/Sam/paros/session/Lates

Paros Scanning Report

Report generated at Sat, 10 Feb 2007 03:30:41.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	2
Informational	0

Alert Detail

Medium (Suspicious)	IIS default file
Description	Microsoft IIS 4.0, 5.0 or 6.0 default files are found.
URL	http://mtsconsulting.net/_vti_bin/_vti_aut/author.dll
URL	http://mtsconsulting.net/_vti_bin/_vti_adm/admin.dll
URL	http://mtsconsulting.net/_vti_bin/shtml.dll
URL	http://mtsconsulting.net/_vti_inf.html
URL	http://mtsconsulting.net/postinfo.html
Solution	Remove default files and virtual directories.

Related organizations

- Companies connected with the target organization may contain details about target organization:
  - Business partners
  - Third party suppliers
  - Customers
- Related companies system may have vulnerabilities which could enable access to target organization systems

Location details

- Location details will enable dumpster diving, social engineering, and other mechanical attacks
- Physical addresses can lead to unauthorized access to buildings, wired and wireless networks, computers, mobile devices etc
- Layout and building plans can be obtained using satellite imagery of location/building
- Google street view can be used to familiarize with the surroundings

Person details

- Social media sites like facebook, linkedin, phonenumber.com, truecaller, twitter.com, classmates.com, monster.com, reunion.com etc can be used to access personal details
- Details can include emai, phone, residential address, date of birth, location changes, pictures of residences etc
- Paid sites available to sell personal data for very low cost - **peoplesearch.com, spokeo.com**
- On-line employee resumes and job posting provide information about technologies in use, location of IT systems etc
- Disgruntled employees stealing and selling information

Search engines

- Google Dorks
  - Microsoft Windows Server with Remote Desktop connection exposed-> allinurl:tsweb/default.htm
- GHDB
- Tools
  - Athena,
  - SiteDigger
  - Wikto
  - FOCA analyses metadata associated with a document
- Maltego is a tool to mine data and link relevant pieces of information on a particular subject.
  - provides the ability to aggregate and correlate information and display the relationships in a graphical form

Internet organization

- Core functions of the Internet are managed by a non-profit organization, the Internet Corporation for Assigned Names and Numbers (ICANN, icann.org)
- ICANN coordinates the assignment of the following identifiers that must be globally unique for the Internet to function:
  - Internet domain names
  - IP address numbers
  - Protocol parameters and port numbers
- Three sub-divisions of ICANN are of interest at this point:
  - Address Supporting Organization (ASO): aso.icann.org
  - Generic Names Supporting Organization (GNSO): gnso.icann.org
  - Country Code Domain Name Supporting Organization (CCNSO): ccnso.icann.org

Internet organization…

- Regional Internet Registries (RIRs) manage, distribute, and register public Internet number resources within their respective regions.
- RIRs allocate IPs to organizations, Internet service providers (ISPs), or, in some cases, National Internet Registries (NIRs) or Local Internet Registries (LIRs) if particular governments require it (mostly in communist countries, dictatorships, etc.)
- There are 5 RIRs
  - APNIC (apnic.net): East Asia, Oceania, South Asia and South East Asia
  - ARIN (arin.net): USA, Canada, Parts of caribbean and Antarctica
  - LACNIC (lacnic.net): Latin America and most of Caribbean
  - RIPE (ripe.net): Europe, Central Asia, Russia and West Asia
  - AfriNIC (afrinic.net): Whole of Africa

Internet organization

innovate achieve lead

- GNSO reviews and develops recommendations on domain-name policy for all generic top-level domains (gTLDs):
  - GNSO is not responsible for domain name registration, but is responsible for the generic top-level domains (for example, .com, .net, .edu, .org, and .info)
  - List of generic top-level domains can be found at iana.org/gtld/gtld.htm.
- CCNSO reviews and develops recommendations on domain-name policy for all country-code top-level domains (ccTLDs):
  - ICANN does not handle domain name registrations.
  - List of country-code top-level domains can be found at iana.org/cctld/cctld-whois.htm.

Internet organization

innovate achieve lead

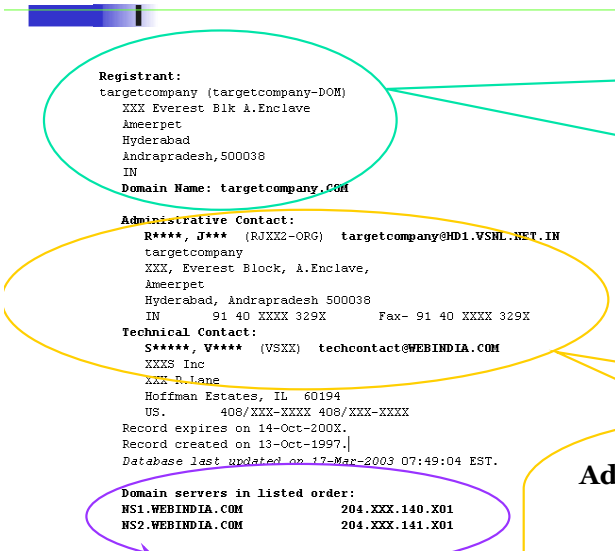
- Some other useful links:
  - iana.org/assignments/ipv4-address-space IPv4 allocation
  - iana.org/assignments/ipv6-address-space IPv6 allocation
  - iana.org/ipaddress/ip-addresses.htm IP address services
  - rfc-editor.org/rfc/rfc3330.txt Special-use IP addresses
  - iana.org/assignments/port-numbers Registered port numbers
  - iana.org/assignments/protocol-numbers Registered protocol numbers

Internet Footprinting tools

- **Whois:** Gathers IP address and domain information
  - whois mit.edu
- **Host:** Can look up one IP address, or the whole DNS Zone file (All the servers in the domain)
  - host mit.edu

```
yourname@S214-01u:~$ nc whois.arin.net 43
18.7.22.69

OrgName:    Massachusetts Institute of Techn
OrgID:      MIT-2
Address:    Room W92-190
Address:    77 Massachusetts Avenue
City:       Cambridge
StateProv:  MA
PostalCode: 02139-4307
Country:    US

NetRange:   18.0.0.0 - 18.255.255.255
CIDR:       18.0.0.0/8
NetName:    MIT
NetHandle:  NET-18-0-0-0-1
Parent:
NetType:    Direct Assignment
NameServer: STRAWB.MIT.EDU
NameServer: W20NS.MIT.EDU
NameServer: BITSY.MIT.EDU
Comment:
RegDate:
Updated:    1998-09-26

RTechHandle: JIS-ARIN
RTechName:   Schiller, Jeffrey
RTechPhone:  +1-617-253-8400
RTechEmail:  jis@mit.edu

OrgTechHandle: JIS-ARIN
OrgTechName:   Schiller, Jeffrey
OrgTechPhone:  +1-617-253-8400
OrgTechEmail:  jis@mit.edu
```

Whois



```
Registrant:
targetcompany (targetcompany-DOM)
   XXX Everest Blk A.Enclave
   Ameerpet
   Hyderabad
   Andrapradesh,500038
   IN
   Domain Name: targetcompany.COM

   Administrative Contact:
      R****, J***  (RJXX2-ORG)  targetcompany@HD1.VSNL.NET.IN
      targetcompany
      XXX, Everest Block, A.Enclave,
      Ameerpet
      Hyderabad, Andrapradesh 500038
      IN       91 40 XXXX 329X       Fax- 91 40 XXXX 329X
   Technical Contact:
      S*****, V****  (VSXX)  techcontact@WEBINDIA.COM
      XXXS Inc
      XXX D.Lane
      Hoffman Estates, IL  60194
      US.       408/XXX-XXXX 408/XXX-XXXX
   Record expires on 14-Oct-200X.
   Record created on 13-Oct-1997.
   Database last updated on 17-Mar-2003 07:49:04 EST.

   Domain servers in listed order:
   NS1.WEBINDIA.COM             204.XXX.140.X01
   NS2.WEBINDIA.COM             204.XXX.141.X01
```

Registrant:
targetcompany (targetcompany-DOM)
Street Address
City, Province
State, Pin, Country
Domain Name: **targetcompany.COM**

Administrative Contact:
Surname, Name (SNIDNo-ORG) t**argetcompany@domain.com**
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Technical Contact:
Surname, Name (SNIDNo-ORG) t**argetcompany@domain.com**
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

```
Domain servers in listed order:
      NS1.WEBHOST.COM              XXX.XXX.XXX.XXX
      NS2.WEBHOST.COM              XXX.XXX.XXX.XXX
```

Nslookup

- Nslookup is a program to query Internet domain name servers.
- Displays information that can be used to diagnose Domain Name System (DNS) infrastructure.
- Helps find additional IP addresses if authoritative DNS is known from whois.
- MX record reveals the IP of the mail server.
- Both Unix and Windows come with a Nslookup client. Third party clients are also available e.g. Sam Spade

Nslookup

- Provides detailed information about IP address associated with a DNS
- Provides what software/tools installed

```
acct18          ID IN A    192.168.230.3
                ID IN HINFO "Gateway2000" "WinWKGRPS"
                ID IN MX    0 exampleadmin-smtp
                ID IN RP    bsmith.rci bsmith.who
                ID IN TXT    "Location:Telephone Room"
ce               ID IN CNAME  aesop
au               ID IN A     192.168.230.4
                ID IN HINFO  "Aspect" "MS-DOS"
                ID IN MX    0 andromeda
                ID IN RP    jcoy.erebus jcoy.who
                ID IN TXT    "Location: Library"
acct21          ID IN A     192.168.230.5
                ID IN HINFO  "Gateway2000" "WinWKGRPS"
```

- To find all systems with Solaris installation

```
[bash]$ grep -i solaris zone_out |wc -l
   388
```

Type of DNS Records

Type	Description
A	A host's IP address. An address record allowing a computer name to be translated into an IP address. Each computer must have this record for it IP address to be located
MX	Host or domain's mail exchange
NS	Host of domain's name server
CNAME	Hosts canonical names – allows additional names or alias to be used to locate a computer
SOA	Indicate authority f domain
SRV	Service location record
RP	Responsible person
PTR	Host domain name – host identified by its IP address
TXT	Generic text record
HINFO	Host information record with CPU type and operating system

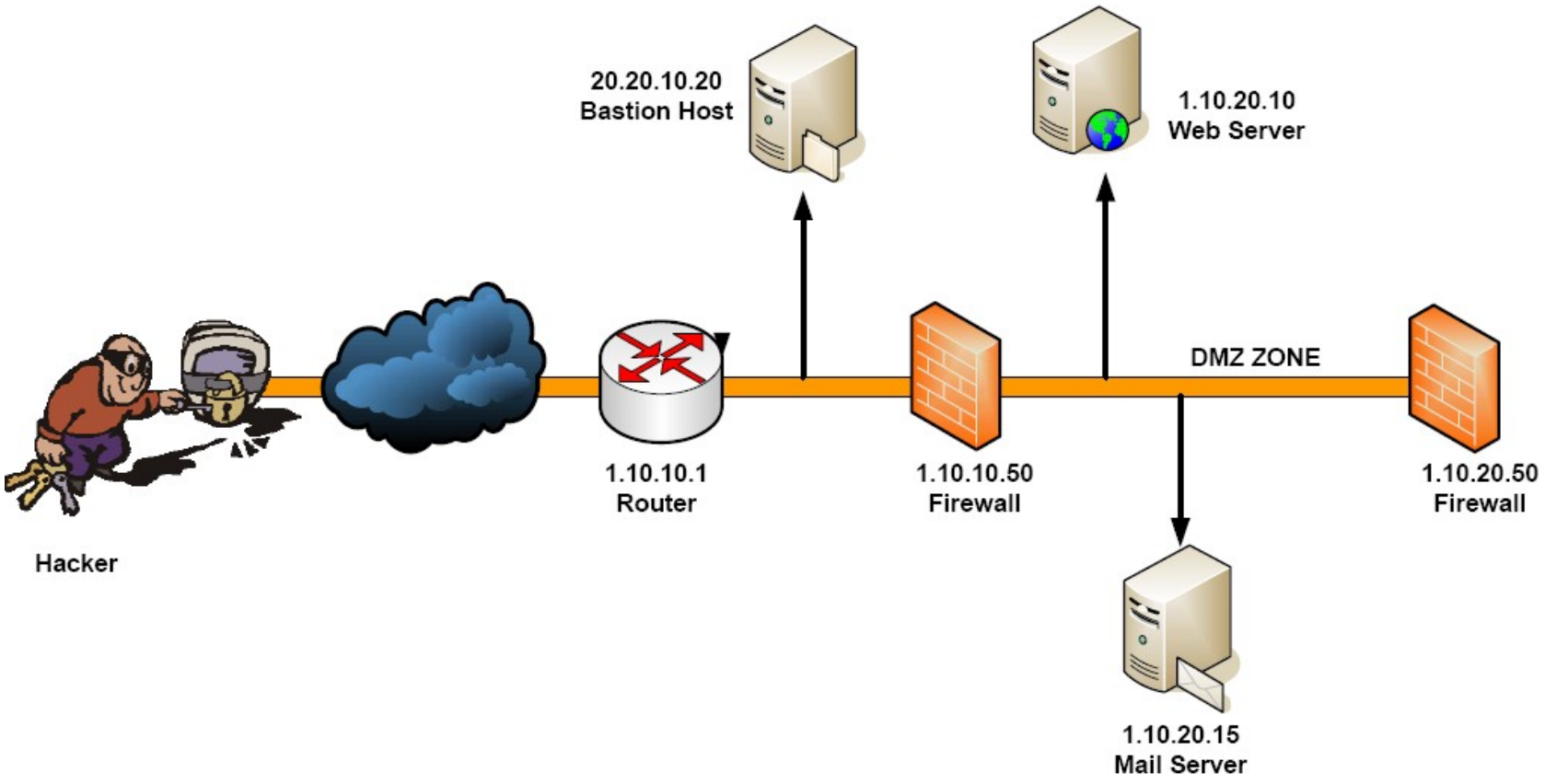
Traceroute

- Traceroute works by exploiting a feature of the Internet Protocol called TTL, or Time To Live.
- Traceroute reveals the path IP packets travel between two systems by sending out consecutive UDP packets with ever-increasing TTLs .
- As each router processes a IP packet, it decrements the TTL. When the TTL reaches zero, it sends back a "TTL exceeded" message (using ICMP) to the originator.
- Routers with DNS entries reveal the name of routers, network affiliation and geographic location.

Traceroute Analysis

- Traceroute can be used to determine the path from source to destination
- Using this information, an attacker can determine the layout of a network and location of devices
- Example: By using the info below an attacker can build a network diagram
  - `traceroute 1.10.10.20, second to last hop is 1.10.10.1`
  - `traceroute 1.10.20.10, third to last hop is 1.10.10.1`
  - `traceroute 1.10.20.10, second to last hop is 1.10.10.50`
  - `traceroute 1.10.20.15, third to last hop is 1.10.10.1`
  - `traceroute 1.10.20.15, second to last hop is 1.10.10.50`

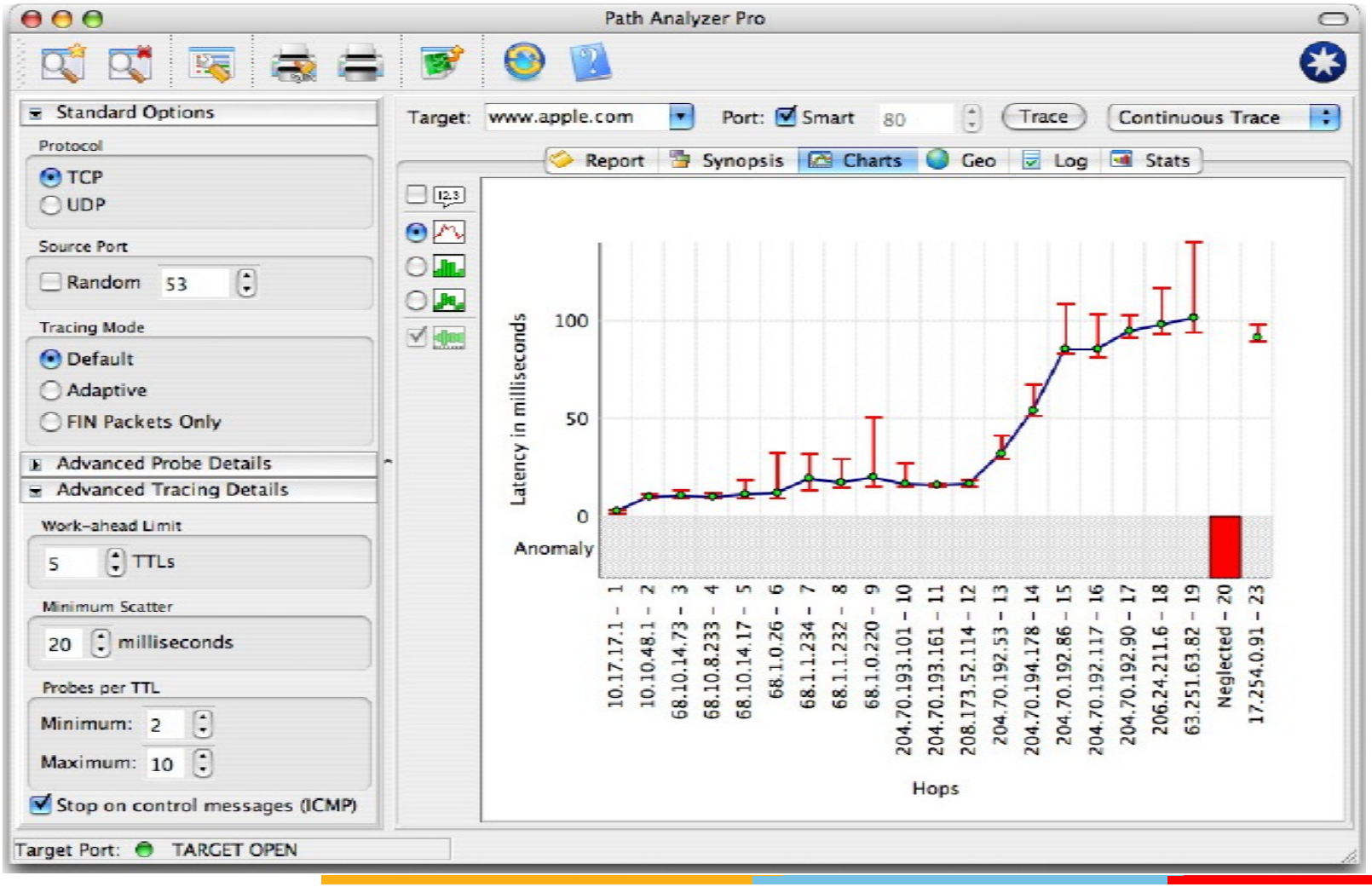
Traceroute Analysis



Path Analyzer Pro

innovate achieve lead

Which severs to focus?



DNS Enumerator

- DNS resolves host name to IP address
- DNS server normally have two instances – primary and secondary
- Provides for redundancy for running DNS in case the primary name server become unavailable
- A zone transfer allows a secondary master server to update its zone database from the primary master
- A misconfigured DNS can allow an untrusted Internet users to perform a DNS zone transfer and see all hosts on a network (needs to be done only by secondary master DNS servers).
- This technique has become almost obsolete but:
  - This vulnerability allows for significant information gathering on a target.
  - It is often the springboard to attacks that would not be present without it.
  - You can still find many DNS servers that allow this feature.

DIG (Domain Information Groper)

- Determine companies primary DNS server
  - Look for the Start of Authority (SOA) record
  - Shows zones or IP addresses
    - dig soa mit.edu
    - Shows three servers, with IP addresses
    - This is a start at mapping the MIT network

```
yourname@S214-01u:~$ dig soa mit.edu

; <<>> DiG 9.3.2 <<>> soa mit.edu
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60742
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;mit.edu.                       IN      SOA

;; ANSWER SECTION:
mit.edu.                4539    IN      SOA     BITSY.mit.edu. NETWOR
it.edu. 4349 3600 900 3600000 21600

;; AUTHORITY SECTION:
mit.edu.                4539    IN      NS      STRAWB.mit.edu.
mit.edu.                4539    IN      NS      BITSY.mit.edu.
mit.edu.                4539    IN      NS      W20NS.mit.edu.

;; ADDITIONAL SECTION:
BITSY.mit.edu.          14362   IN      A       18.72.0.3
W20NS.mit.edu.          16061   IN      A       18.70.0.160
STRAWB.mit.edu.         12793   IN      A       18.71.0.151
```

DNS Interrogation – host & dig

- host provides list of IP address

```
host -l example.com
and
host -l -v -t any example.com

host -l example.com |cut -f 4 -d"" "" >\> /tmp/ip_out
```

- DIG provides similar details
- dnsrecon (github.com/darkoperator/dnsrecon) transfers zone information recursively. To run dnsrecon use following commands

```
[bash]$ python dnsrecon.py -x -d internaldomain.com
[*] Performing General Enumeration of Domain: internaldomain.com
[-] Wildcard resolution is enabled on this domain
[-] It is resolving to 10.10.10.5
[-] All queries will resolve to this address!!
[*] Checking for Zone Transfer for internaldomain.com name servers
[*] Trying NS server 10.10.10.1
[*] Zone Transfer was successful!!
```

- Other scripts available for DNS enumeration are: dnsenum, dnsmap, fierce

SpiderFoot

- Free, open source, domain footprinting tool which scrapes the websites on a specified domain and searches Google, Netcraft, Whois, and DNS to build a profile of:
  - Sub-domains
  - Affiliates
  - Web server versions
  - Users
  - Similar domains
  - Email addresses
  - Netblocks

Cookies

- Cookie
  - Text file generated by a Web server
  - Stored on a user's browser
  - Information sent back to Web server when user returns
  - Used to customize Web pages
  - Some cookies store personal information: Security issue
- View cookies (Chrome): Website -> Inspect -> Application -> Cookies

Social Engineering

- Targets the human component of a network to obtain confidential personal information (passwords, email, phone etc)
- Main idea:
  - "Why to crack a password when you can simply ask for it?"
  - Users divulge their passwords to IT personnel
- Tactics: Persuasion, Intimidation, Coercion, Extortion, Blackmailing
- Biggest and most difficult security threat to networks
- Recognize personality traits and understand to read body language
- Techniques: Urgency, Quid-pro-quid, Status-quo, Kindness, Position
- Prevention:
  - Train user not to reveal any information to outsiders
  - Verify caller identity: ask questions, call back to confirm
  - Security drills

Dumpster Diving

- Attacker finds information in victim's trash
  - Discarded computer manuals: Notes or passwords written in them
  - Telephone directories
  - Calendars with schedules
  - Financial reports
  - Inter-office memos
  - Company policy
  - Utility bills
  - Resumes of employees
- Prevention
  - Educate your users about dumpster diving
  - Proper trash disposal
  - Use "disk shredder" software to erase disks before discarding them
    - Software writes random bits
    - Done at least seven times
  - Discard computer manuals offsite
  - Shred documents before disposal

List of Footprinting Tools

- Whois & SmartWhois
- Nslookup
- ARIN
- Neo Trace
- Visual Route Trace
- Path Analyzer Pro
- EmailTrackerPro
- Email Spider
- Geo Spider
- Website Watcher
- HTTrack Web Copier
- Google Earth

How to setup a fake website

- Mirror the entire website from a target URL
- Register a fake domain name which sound like the real website
- Host the mirrored website into fake website URL
- Send phishing e-mails to the victims directing to the fake website
- Continuously update fake mirror website with real website

How to setup a fake website

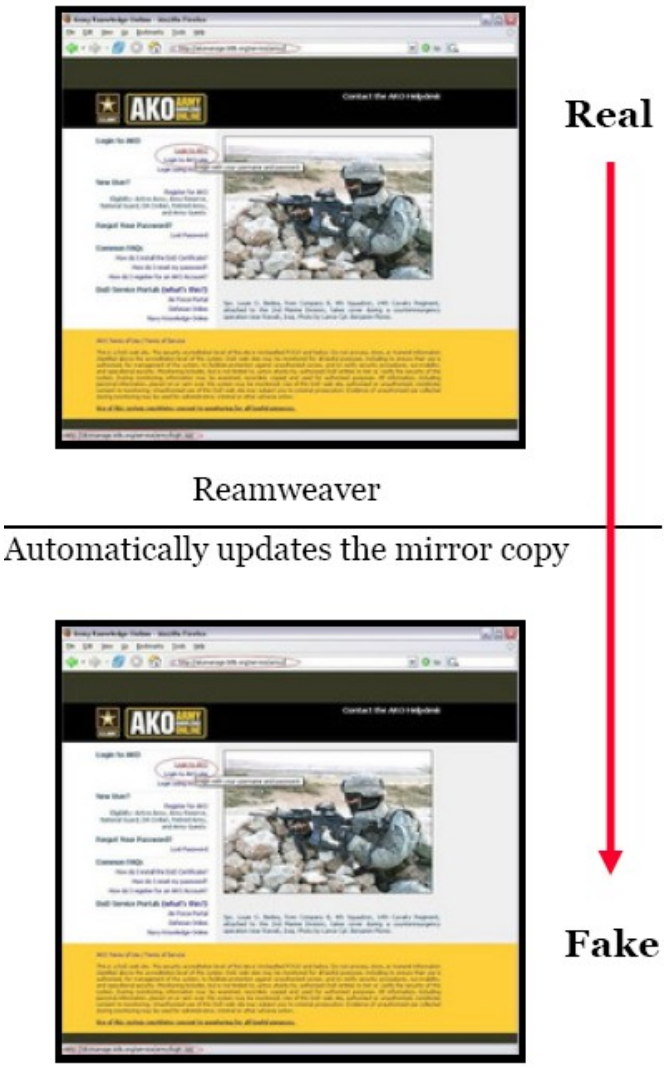
innovate achieve lead

Real Website

Fake Website

How to setup a fake website

- Reamweaver has everything you need to instantly “steal" anyone's website, copying the real-time "look and feel" but letting you change any words, images, etc. that you choose
- When a visitor visits a page on your stolen (mirrored) website, Reamweaver gets the page from the target domain, changes the words as you specify, and stores the result (along with images, etc.) in the fake website
- With this tool your fake website will always look current, Reamweaver automatically updates the fake mirror when the content changes in the original website
- Download: http://www.eccouncil.org/cehtools/reamweaver.zip



Scanning

Scanning

- Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network.
- Network scanning is used to create a profile of the target organization.
- Scanning is used to collect more information using complex and aggressive reconnaissance techniques.
- Vulnerability scanning is performed by pen-testers to detect the possibility of network security attacks.
- This technique led hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication, or weak encryption algorithms.

Scanning Types

- Network scanning
- Port scanning
- Vulnerability scanning

Network Scanning

innovate achieve lead

- Objectives
  - To discover live hosts/computer, IP address, and open ports of the victim.
  - To discover services that are running on a host computer.
  - To discover the Operating System and system architecture of the target.
  - To discover and deal with vulnerabilities in Live hosts.
- Methods
  - Hackers and Pen-testers check for Live systems.
  - Check for open ports (also known as Port Scanning)
  - Scanning beyond IDS (Intrusion Detection System)
  - Banner Grabbing: method for obtaining information regarding the targeted system on a network and services running on its open ports. Telnet and ID Serve are the tools used mainly to perform a Banner-grabbing attack.
  - Scan for vulnerability
  - Prepare Proxies

Port Scanning

- It is a conventional technique used by penetration testers and hackers to search for open doors from which hackers can access any organization's system.
- During this scan, hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system, and the targeted organization's topology.
- Once the Hacker fetches the victim organization's IP address by scanning TCP and UDP ports, the Hacker maps this organization's network under his/her grab.
- Amap is a tool to perform port scanning.

Port Scanning Techniques

- **SYNScan**: SYN scan or stealth doesn't complete the TCP three-way handshake. A hacker sends an SYN packet to the target, and if an SYN/ACK frame is received back, the port is in a position to listen. If an RST is retrieved from the target, the port is closed or not activated.
- **XMASScan**: XMAS scan send a packet which contains URG (urgent), FIN (finish) and PSH (push) flags. If there is an open port, there will be no response; but the target responds with an RST/ACK packet if the port is closed. (RST=reset).
- **FINScan**: A FIN scan is similar to an XMAS scan except that it sends a packet with just the FIN (finish) flag and no URG or PSH flags. FIN scan receives the same response and has the same limitations as XMAS scans.
- **IDLEScan**: An IDLE scan uses a spoofed/hoax IP to send the SYN packet to the target by determining the port scan response and IP header sequence number.
- **Inverse TCP Flag Scan:** Attacker sends TCP probe packets with a TCP flag (FIN, URG PSH) or no flags. If there is no response, it indicates that the port is open, and RST means it is closed.
- **ACK Flag Probe Scan:** Attacker sends TCP probe packets where an ACK flag is set to a remote device, analyzing the header information (TTL and WINDOW field). The RST packet signifies whether the port is open or closed.

Vulnerability Scanning

- Proactive identification of the system's vulnerabilities within a network in an automated manner to determine whether the system can be exploited.
- Tools:
  - **Nmap**: extract information such as live hosts on the network, services, type of packet filters/firewalls, operating systems, and OS versions.
  - **Angry IP Scanner**: scans for systems available in a given input range.
  - **Hping2/Hping3**: are command-line packet crafting and network scanning tools used for TCP/IP protocols.
  - **Superscan**: is another powerful tool developed by Mcafee, which is a TCP port scanner, also used for pinging.
  - **ZenMap**: is another very powerful Graphical user interface (GUI) tool to detect the type of OS, OS version, ping sweep, port scanning, etc.
  - **Net Scan Tool Suite Pack**: is a collection of different types of tools that can perform a port scan, flooding, webrippers, mass emailers etc
  - **Wireshark and Omnipeak** are two powerful and famous tools that listen to network traffic and act as network analyzers.
  - Other PCs tools: Advanced Port Scanner, Net Tools, MegaPing, CurrPorts, PRTG Network Monitor, SoftPerfect Network Scanner, Network Inventory Explorer etc.

Thank You