sait.ca

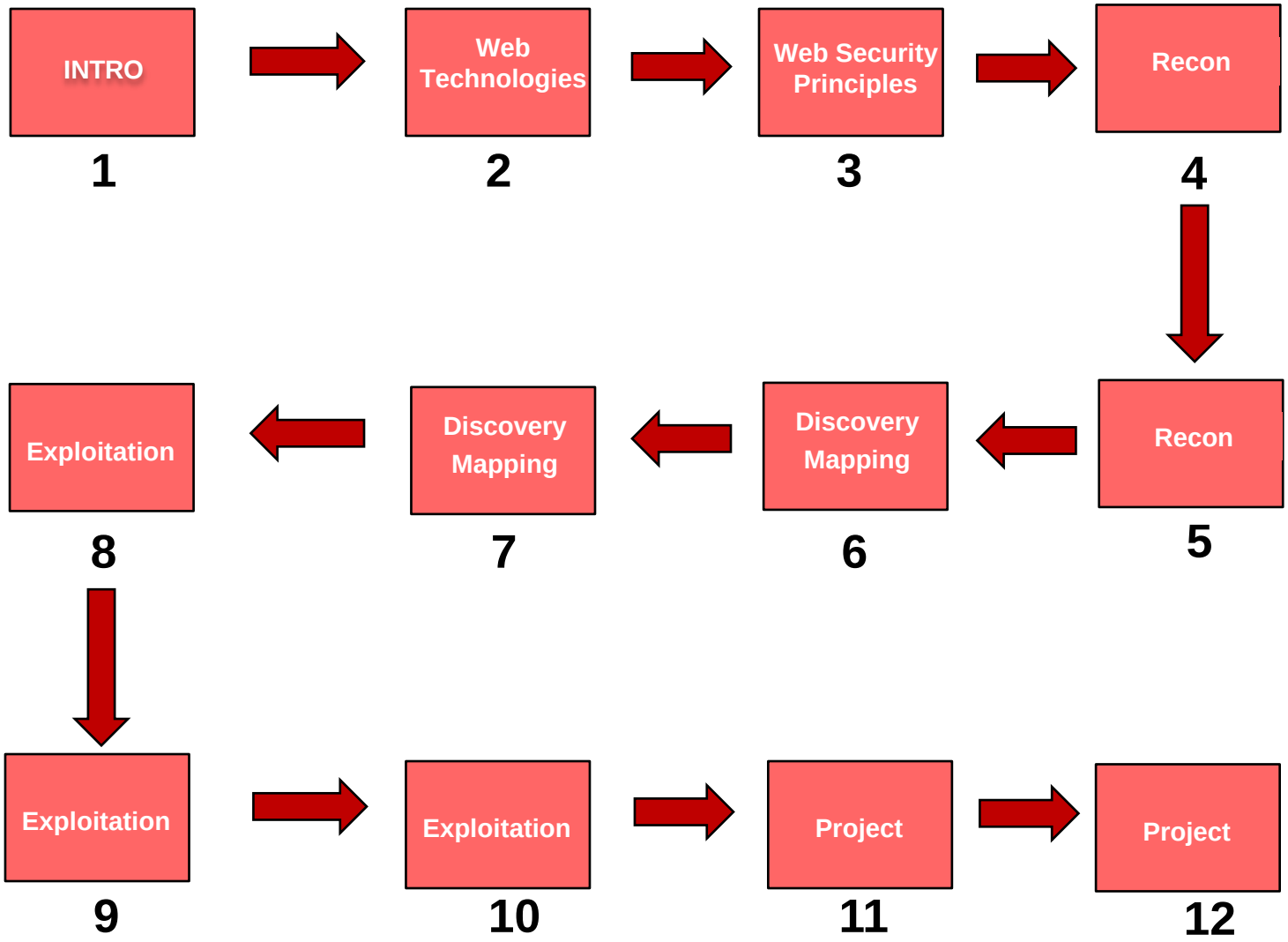
SAIT POLYTECHNIC

FURTHER YOUR PASSION

Web App & Data Base Security

Recon

Web App & Data Base Security



Agenda

- Reconnaissance;
- Information Gathering;
- Passive and Active tools;
- Mapping;
- Project: Phase 1: Recon and Mapping.

Reconnaissance

Reconnaissance

- Phase one of four in our web app penetration testing methodology;
  - It guides the attacks as the test moves forward.
- Easily the most critical step of the test;
- Results may help providing insight for improving security practices;
  - Google searches and groups;
  - DNS tools;
  - ICMP tools.

Target Selection: Defining the test scope

Reconnaissance

- Pen-testers need to know the targets:
  - Could be target servers, indicated by individual IP address, IP ranges or/and domain names;
  - Target could be application, on single server or in different servers
- The target information could be gathering from:
  - Information provided by the company that is hiring you;
  - Internal team who supports the applications;
  - Processes.

Identifying Target Machines

- Which machines are interesting and part of the target application and systems;
- This includes infrastructure devices:
  - Load balancers;
  - SSL offload devices;
  - Web App Firewalls;
  - Proxies.
- Information here will help guide the attacks:
  - Vulnerabilities in the host;
  - Commands supported by the host.

Information Gathering

It is the preliminary activity in which an attacker attempts to gather information about the a target preparatory to launching an attack.

- **Passive Information gathering:** it is used to gain information about the target without having any physical connectivity or access to it. **Domain names, IPs, location or servers** and, etc.;
- **Active Information gathering:** a logical connection is setup with the target in order to gain information. It probes the network to acquire information about operating systems, available services, open ports, routers and hosts;

Information Gathering – 7 Steps

Reconnaissance

7 steps of the information gathering process

- **Step 1:** Gathering information;
- **Step 2:** Locating the network range;
- **Step 3:** Identifying active machines;
- **Step 4:** Finding open ports and applications;
- **Step 5:** Detecting operating systems;
- **Step 6:** Fingerprinting services;
- **Step 7:** Mapping the network.

Passive Information Gathering - whois

Reconnaissance

whois: searches for DNS information / Identifies the owner of the domain of IP addresses

Syntax

#whois domain.com

EXAMPLE

[root@sait tmp]# whois sait.ca

```
root@bt: ~
;; AUTHORITY SECTION:
pe.senai.br.            300     IN      SOA     calhetas.pe.senai.br. root.pe.senai.br. 2010

;; Query time: 228 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Fri Nov 23 15:49:46 2012
;; MSG SIZE  rcvd: 83

root@bt:~# whois sait.ca
Domain name:            sait.ca
Domain status:          registered
Creation date:          2000/10/16
Expiry date:            2019/12/01
Updated date:           2011/06/02

Registrar:
    Name:               Webnames.ca Inc.
    Number:             70

Registrant:
    Name:               Southern Alberta Institute of Technology

Administrative contact:
    Name:               Gary MacDonald
    Postal address:     Information Systems
                        1301 North West 16 Avenue
                        Calgary AB T2M 0L4 Canada
    Phone:              1 403 2848370
    Fax:                1 403 2848811
    Email:              domain.name.administrators@sait.ca

Technical contact:
    Name:               Lorraine Kramer
    Postal address:     Information Systems
                        1301 North West 16 Avenue
                        Calgary AB T2M 0L4 Canada
    Phone:              1 403 2848066
    Fax:                1 403 2848811
    Email:              [illegible]s@sait.ca

Name servers:
    ns701.sait.ca       142.110.131.2
    ns702.sait.ca       142.110.131.254

% WHOIS look-up made at 2012-11-23 20:51:20 (GMT)
%
% Use of CIRA's WHOIS service is governed by the Terms of Use in its Legal
% Notice, available at http://www.cira.ca/legal-notice/?lang=en
%
% (c) 2010 Canadian Internet Registration Authority, (http://www.cira.ca/)
root@bt:~#
```

Name servers:

ns701.sait.ca	**142.110.131.2**
ns702.sait.ca	**142.110.131.254**

Passive Information Gathering - Dig

Reconnaissance

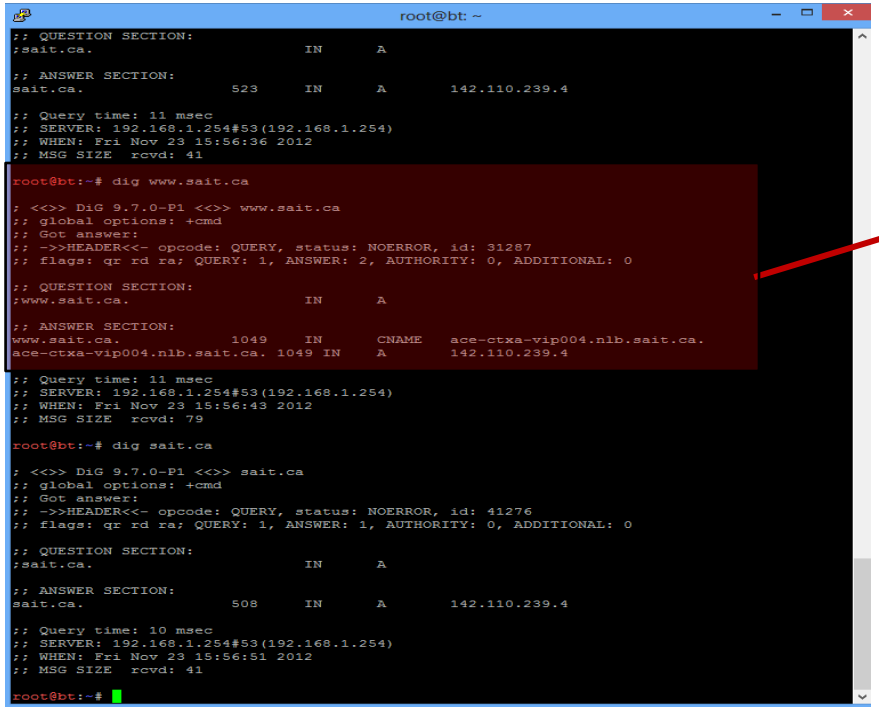
dig: DNS lookup utility / will attempt to capture all DNS records with a zone transfer.

Syntax

#dig domain.com

EXAMPLE

[root@sait tmp]# dig www.sait.ca



;; ANSWER SECTION:

www.sait.ca. 1049 IN CNAME ace-ctxa-vip004.nlb.sait.ca.

ace-ctxa-vip004.nlb.sait.ca. 1049 IN A 142.110.239.4

Passive Information Gathering - Nslooup

Reconnaissance

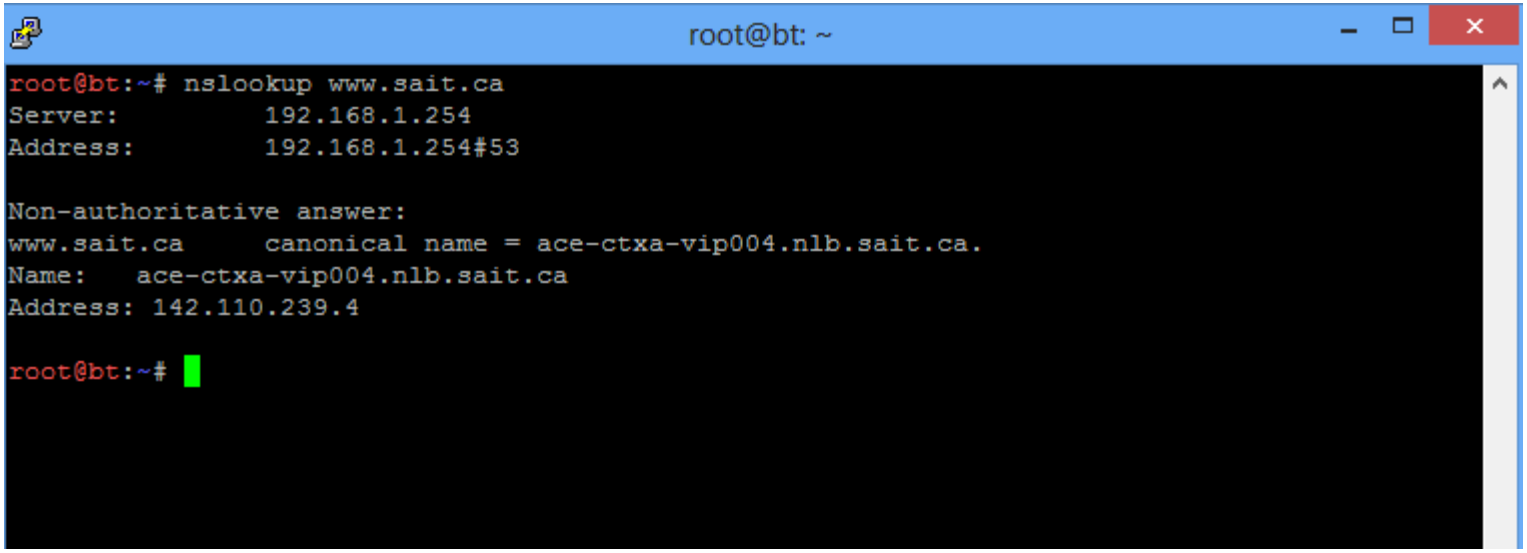
nslookup: query Internet name servers interactively

Syntax

#nslookup domain.com

EXAMPLE

[root@sait tmp]# nslookup www.sait.ca



Passive Information Gathering – The Harvest

Reconnaissance

The Harvest: it is a script that allows us to quickly catalog both email addresses and subdomains that are directly related to our target.

- Found on: root@bt:/pentest/enumeration/theharvester/

Syntax

#./theHarvester.py [options] target_domain.com [options] public_repository

EXAMPLE

[root@sait tmp]# ./theHarvester.py -d sait.ca -l 10 -b google

- -d: specify the target domain name
- -l: used to limit the number of results
- -b: search engine

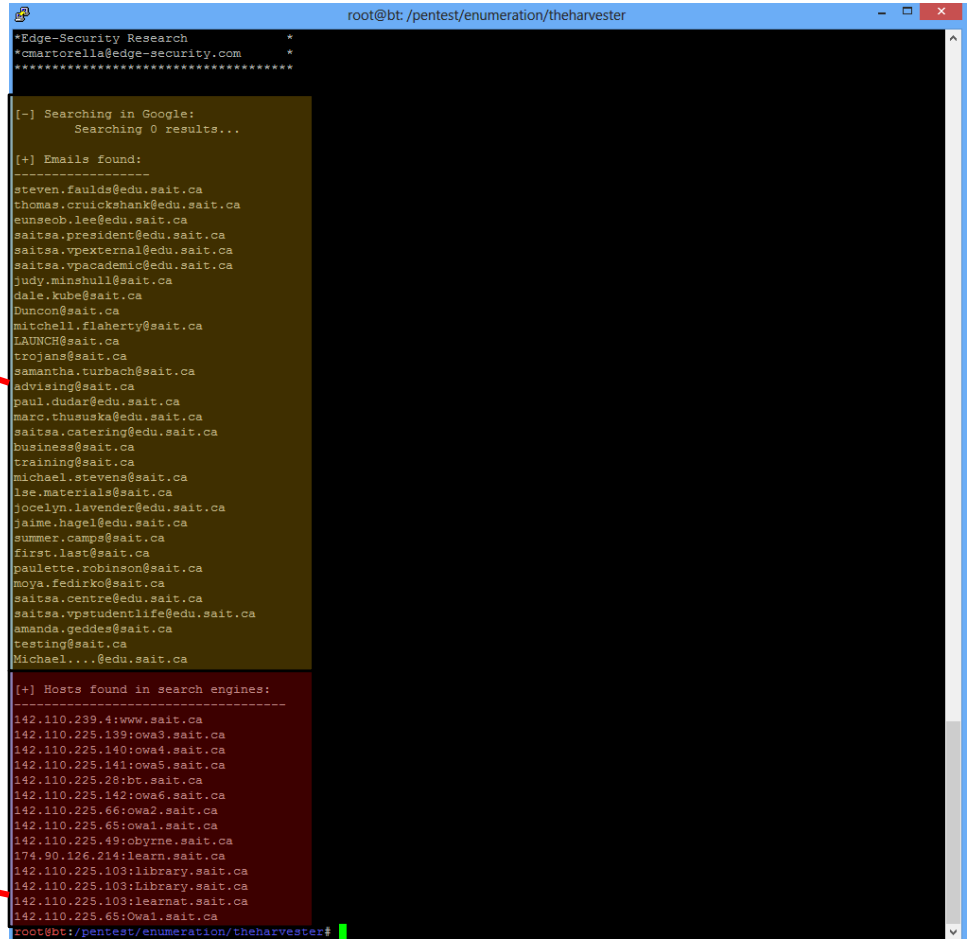
Passive Information Gathering – The Harvest

Reconnaissance

The Harvest: Results

Emails / Email Format that could be used on phishing attempts

More IP addresses/ranges to be scanned.

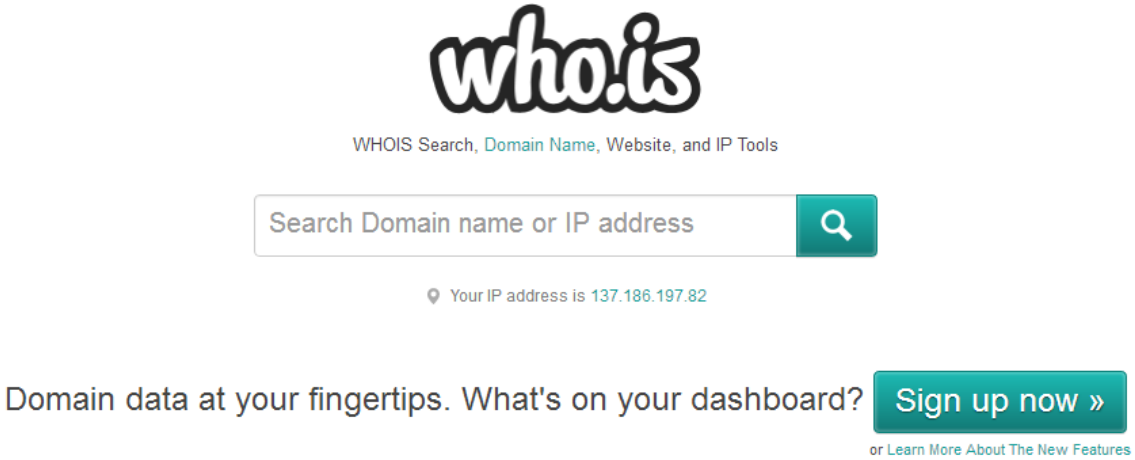


Passive Information Gathering - Tools

Reconnaissance

Third-party website:

- **http://who.is;**
- **http://www.dnsstuff.com/;**
- **http://www.betterwhois.com/.**



Passive Information Gathering – Search Engines

Reconnaissance

- Search engines are the best source of data around;
- Amazingly effective due to the amounts of information people reveal purposely or inadvertently.

Passive Information Gathering – Google Hacking

Reconnaissance

GOOGLE-HACKING (Google Dork): is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use

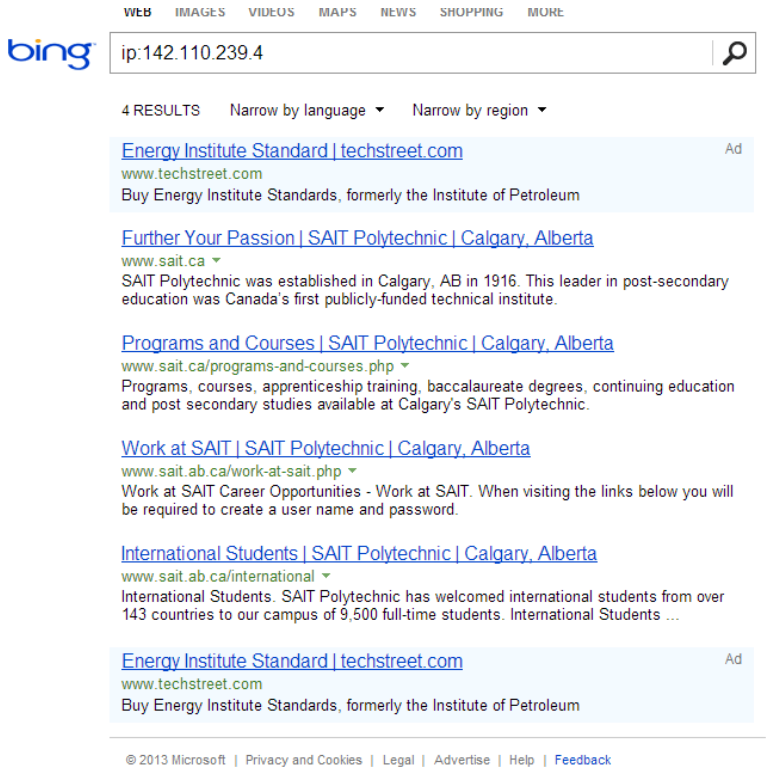
- www.sait.ca filetype:xls
- www.sait.ca filetype:pdf
- site:www.sait.ca filetype:db

Operator	Purpose
intitle	Search page Title
allintitle	Search page title
inurl	Search URL
allinurl	Search URL
filetype	specific files
allintext	Search text of page only
site	Search specific site
link	Search for links to pages
inanchor	Search link anchor text
numrange	Locate number
daterange	Search in data range
author	Group author search
group	Group name search
insubject	Group subject search
msgid	Group msgid search

Passive Information Gathering - Bing

Reconnaissance

- Bing offers a search modifier that shows sites on a single address:
  - **IP:142.110.239.4** will find all the sites with this IP.



Passive Information Gathering – Press Release and Job Posting

Reconnaissance

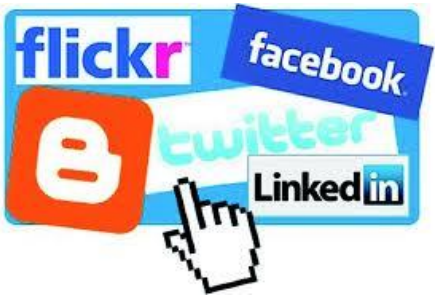
Press Releases and Job Posting

- Press releases are a great source of information:
  - Business announcements reveal projects and new technologies;
  - Vendors commonly announce their big, brand-name clients.
- Job Posting:
  - Discover technologies supported by the company;
  - May show gaps in knowledge since they are either needing support people for new tech.

Passive Information Gathering – Social Networking

Reconnaissance

- Social Networks are one of the more popular destinations of the web;
- Many site allow for searching based on company name;
- Lots of information is disclosed on there sites;
  - Personal for social engineering attacks;
  - Answers to password reset questions.



Active Information Gathering – ICMP Tools

Reconnaissance

Target discovery

ping: checks if the particular host is available

Syntax

#ping IP_ADDRESS

EXAMPLE

[root@sait tmp]# ping 10.2.2.1

traceroute: print the route packets trace to network host

Syntax

#traceroute IP_ADDRESS

```
root@bt# traceroute 10.2.2.1
traceroute to 10.2.2.1 (10.2.2.1), 30 hops max, 60 byte packets
 1  10.2.2.1 (10.2.2.1)  0.297 ms  0.164 ms  0.146 ms
```

Active Information Gathering - Arping

Reconnaissance

Target discovery

arping: sends arp and/or ip pings to a given host. Checks if the host is in use on the network.

Syntax

#arping IP_ADDRESS

```
EXAMPLE
[root@sait tmp]# arping 10.2.2.1
ARPING 10.2.2.1
60 bytes from 00:0c:29:08:3e:0d (10.2.2.1): index=0 time=11.000 usec
60 bytes from 00:0c:29:08:3e:0d (10.2.2.1): index=1 time=5.000 usec
60 bytes from 00:0c:29:08:3e:0d (10.2.2.1): index=0 time=11.000 usec
60 bytes from 00:0c:29:08:3e:0d (10.2.2.1): index=1 time=5.000 usec
```

Active Information Gathering - Fping

Target discovery

fping: sends arp and/or ip pings to a given host. Checks if the host is in use on the network.

Syntax

#fping IP_ADDRESS

```
EXAMPLE
[root@sait tmp]# fping 10.2.2.1 10.2.2.3 10.2.2.4
10.2.2.1 is alive
ICMP Host Unreachable from 10.2.2.30 for ICMP Echo sent to 10.2.2.4
10.2.2.3 is unreachable
```

> Backtrack | Information Gathering | Network Analysis | Identify Live Hosts

Active Information Gathering - Genlist

Reconnaissance

Target discovery

genlist: tool can be used to get a list of hosts that respond to the ping probes (ping scanner).

Syntax

#genlist IP_Information

```
EXAMPLE
[root@sait tmp]# genlist –s 192.168.1.\*
192.168.1.64
192.168.1.65
192.168.1.66
192.168.1.69
```

Active Information Gathering – hping3

Reconnaissance

Target discovery

hping3: send arbitrary TCP/IP packets to network hosts. Sends custom packets and to display replies from the target.

Syntax

#hping3 [options] IP_Address

```
EXAMPLE
[root@sait tmp]#  hping3 -c 2 10.2.2.1
HPING 10.2.2.1 (eth1 10.2.2.1): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=10.2.2.1 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=0.2 ms
len=46 ip=10.2.2.1 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=0.4 ms
```

> Backtrack | Information Gathering | Network Analysis | Identify Live Hosts

Active Information Gathering - Nping

Target discovery

nping: Network packet generation tool (TCP, UDP, ICMP, ARP) / ping utility.

Syntax

#nping [options] IP_Address

EXAMPLE

[root@sait tmp]# nping -c 1 --tcp -p 80 --flags syn 10.2.2.1

SENT (0.0031s) TCP 10.2.2.30:14988 > 10.2.2.1:80 **S** ttl=64 id=3213 iplen=40 seq=1836200572 win=1480

RCVD (0.0038s) TCP 10.2.2.1:80 > 10.2.2.30:14988 **SA** ttl=64 id=0 iplen=44 seq=3156447310 win=5840 <mss 1460>

nping_event_handler(): TIMER killed: Resource temporarily unavailable

Note: S = SYN and SA = SYN-ACK, the target has port 80 open.

> Backtrack | Information Gathering | Network Analysis | Identify Live Hosts

Active Information Gathering - Nping

Target discovery

nping: Network packet generation tool (TCP, UDP, ICMP, ARP) / ping utility.

Syntax

#nping [options] IP_Address

EXAMPLE

[root@sait tmp]# nping -c 1 --tcp -p 8080 --flags syn 10.2.2.1

SENT (0.0041s) TCP 10.2.2.30:13280 > 10.2.2.1:8080 **S** ttl=64 id=3773 iplen=40 seq=1614043183 win=1480

RCVD (0.0047s) TCP 10.2.2.1:8080 > 10.2.2.30:13280 **RA** ttl=64 id=0 iplen=40 seq=0 win=0

Note: S = SYN and RA = RST-ACK, it does not have port 8080 open.

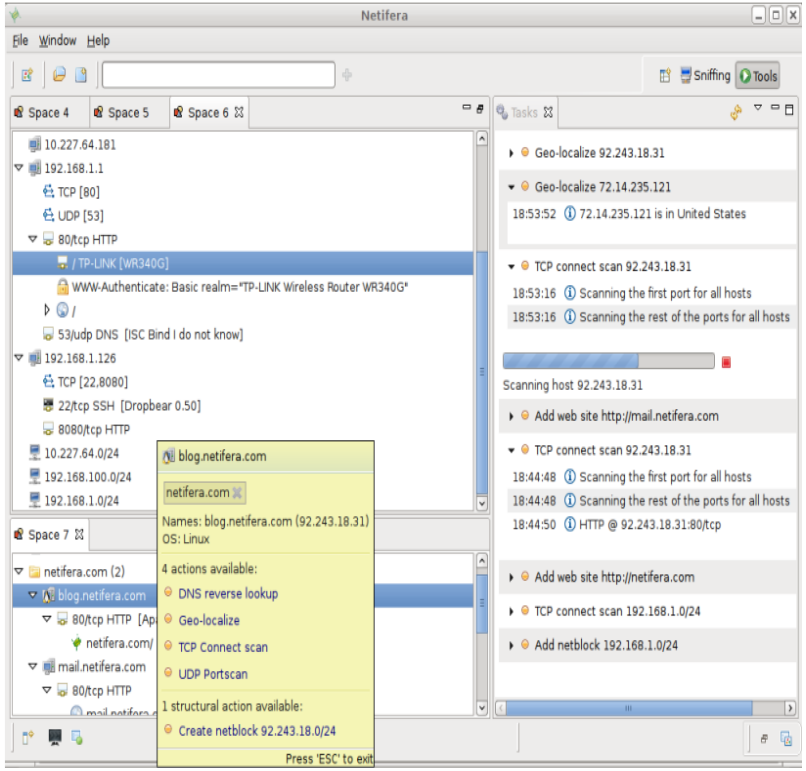
> Backtrack | Information Gathering | Network Analysis | Identify Live Hosts

Active Information Gathering – Port Scanning

Reconnaissance & Mapping

NETIFERA: it is a network security tool to provide:

- Network scanning and services detection;
- Identifying operating system;
- Brute-force DNS name;
- Carrying out DNS zone transfer;
- Discovery web application.



> Backtrack | Information Gathering | Network Analysis | Identify Live Hosts

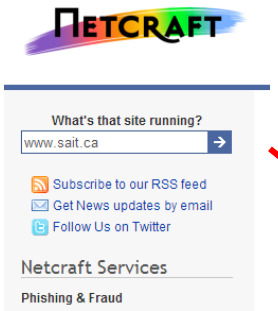
Server Version

- Web Servers are a main target of the test:
  - But they are not the only target. Data bases and client systems should be considered too.
- The server type and version significantly affects the test:
  - May be vulnerable to a misconfiguration attack;
  - Different server types can impact the attack methods;

Passive Information Gathering - Netcraft

Reconnaissance

NETCRAFT: it will return information about your target in regards to IPs, websites it is aware of that contain your search words.



Site	http://www.sait.ca	**Last reboot**	unknown Uptime graph
Domain	sait.ca	**Netblock owner**	Southern Alberta Institute of Technology
IP address	142.110.239.4	**Site rank**	1895115
Country	CA	**Nameserver**	ns701.sait.ca
Date first seen	September 2012	**DNS admin**	postmaster@sait.ca
Domain Registrar	unknown	**Reverse DNS**	sait.ab.ca
Organisation	unknown	**Nameserver Organisation**	unknown
Check another site:			

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
Southern Alberta Institute of Technology Calgary AB CA	142.110.225.22	Windows 2000	Microsoft-IIS/5.0	5-Apr-2011
Southern Alberta Institute of Technology Calgary AB CA	142.110.225.22	Windows 2000	Microsoft-IIS/5.0	26-Mar-2009
Southern Alberta Institute of Technology Calgary AB CA	142.110.225.22	Windows 2000	Microsoft-IIS/5.0	25-Aug-2008
Southern Alberta Institute of Technology Calgary AB CA	142.110.225.22	Windows 2000	Microsoft-IIS/5.0	31-Jan-2008
Southern Alberta Institute of Technology Calgary AB CA	142.110.225.22	Windows 2000	Microsoft-IIS/5.0	10-Aug-2007
Southern Alberta Institute of Technology Calgary AB CA	142.110.225.22	Windows 2000	Microsoft-IIS/5.0	13-Jan-2005
Southern Alberta Institute of Technology Calgary AB CA	142.110.225.22	NT4/Windows 98	Microsoft-IIS/4.0	30-Aug-2004
Southern Alberta Institute of Technology Calgary AB CA	142.110.131.192	NT4/Windows 98	Microsoft-IIS/4.0	25-Apr-2002

Active Information Gathering - Amap

Service Enumeration

AMAP: it can be used to check the application that is running on a specific port (Application Map).

Syntax

#amap [options] IP_Address Port

EXAMPLE

[root@sait tmp]# amap -bq 10.2.2.1 80

/>\n \n<hr>\n<address>**Apache/2.2.8** (Ubuntu)

Protocol on 10.2.2.1:80/tcp matches http-apache-2 - banner: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n<html><head>\n<title>400 Bad Request</title>\n</head><body>\n<h1>Bad Request</h1>\n Your browser sent a request that this server could not understand.
\n \n<hr>\n<address>**Apache/2.2.8** (Ubuntu)

> Backtrack | Information Gathering | Network Analysis | Service Fingerprinting

Information Gathering - HTTPrint

Mapping

Service Enumeration

HTTPRINT: it can be used to detect an HTTP service software and version (web server fingerprinting tool).

Syntax

#httprint [options] IP_Address –s signatures.txt

```
EXAMPLE
root@bt:/pentest/enumeration/web/httprint/linux# ./httprint -h 10.2.2.1 -s signatures.txt
Finger Printing on http://10.2.2.1:80/
Finger Printing Completed on http://10.2.2.1:80/
--------------------------------------------------
Host: 10.2.2.1
Derived Signature:
Apache/2.2.8 (Ubuntu) DAV/2
```

> Backtrack | Information Gathering | Network Analysis | Service Fingerprinting

Information Gathering - HTTSquash

Mapping

Service Enumeration

HTTSQUASH: it can be used to detect an HTTP service software and version.

Syntax

#httsquash [options] IP_Address

EXAMPLE

root@bt:/pentest/scanners/httsquash# ./httsquash -r 10.2.2.1

FOUND: 10.2.2.1 80

HTTP/1.1 200 OK

Server: **Apache/2.2.8** (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Content-Length: 891

Content-Type: text/html

> Backtrack | Information Gathering | Network Analysis | Service Fingerprinting

Active Information Gathering - Netcat

Mapping

Netcat (NC): Swiss army knife of network connections.

Syntax #nc [options] IP_Address port

EXAMPLE

[root@sait tmp]# nc –vv metasploitable.sait230.ca 80

GET HEAD / 1.0

TEST

TEST

Web server version

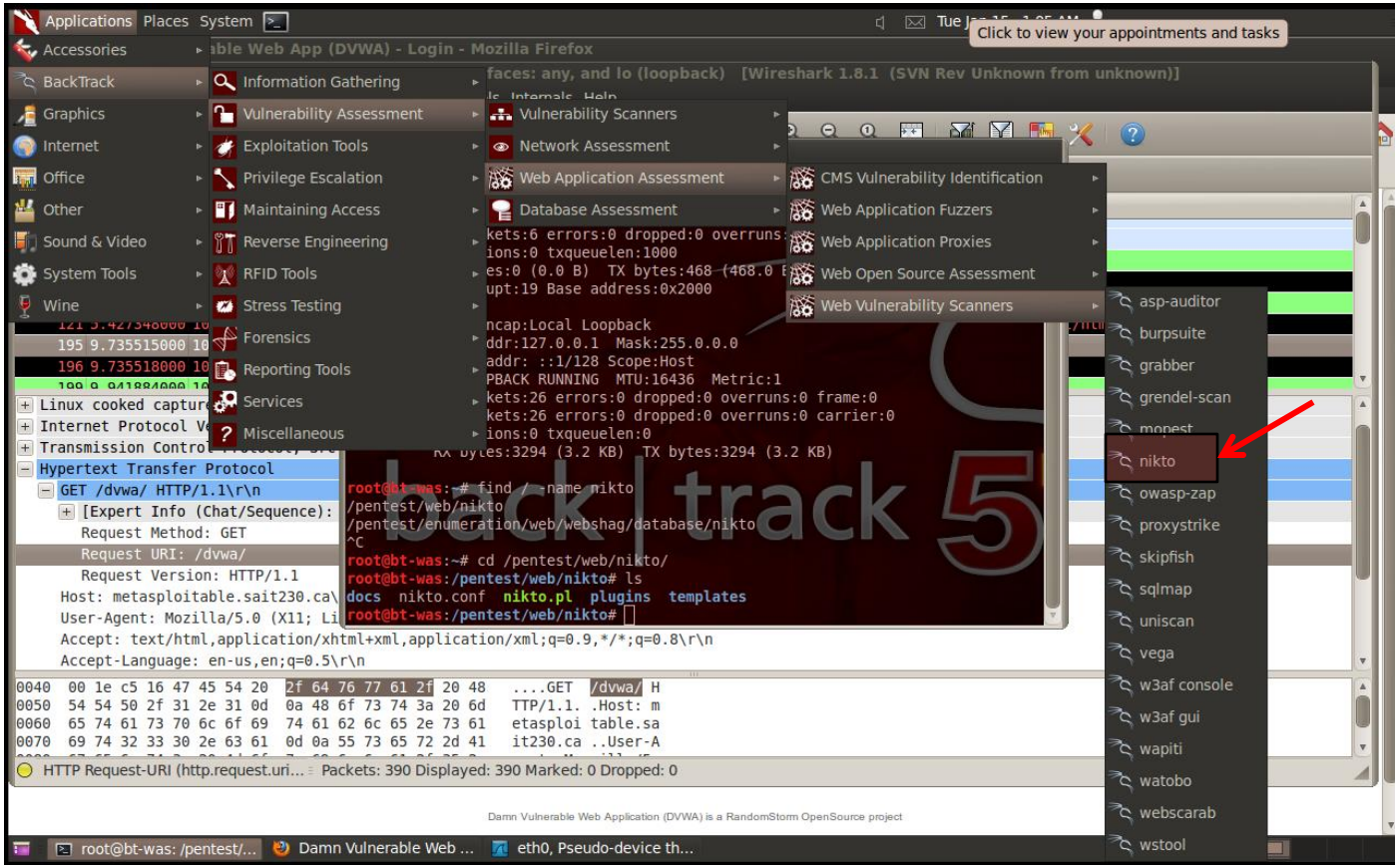
```
root@bt-was:/pentest/web/nikto# nc -vv metasploitable.sait230.ca 80
metasploitable.sait230.ca [10.2.1.1] 80 (www) open
GET HEAD / 1.0
RCUNHA
RCUNHA
HTTP/1.1 400 Bad Request
Date: Fri, 11 Jan 2013 00:21:07 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Content-Length: 395
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Request header field is missing ':' separator.<br />
<pre>
RCUNHA</pre>
</p>
<hr>
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at metasploitable.localdomain Port 80</address>
</body></html>
 sent 29, rcvd 582
```

Active Information Gathering - Nikto

Mapping

NIKTO: a web server vulnerability scanner



Found on:#pentest/web/nikto

Active Information Gathering - Nikto

Mapping

NIKTO: a web server vulnerability scanner

Syntax

:/pentest/web/nikto# ./nikto.pl [options] hostname

EXAMPLE

[root@sait /pentest/web/nikto]#./nikto.pl –host metasploitable.ca

Web server version

```
root@bt-was: /pentest/web/nikto
File  Edit  View  Terminal  Help
docs  nikto.conf  nikto.pl  plugins  templates
root@bt-was:/pentest/web/nikto# ./nikto.pl -host metasploitable.sait230.ca
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.2.1.1
+ Target Hostname:    metasploitable.sait230.ca
+ Target Port:        80
+ Start Time:         2013-01-15 01:08:20 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.19). Apach
e 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microso
ft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
potentially sensitive information via certain HTTP requests that contain specifi
c QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databa
ses, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/: phpMyAdmin is for managing MySQL databases, and shou
ld be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
```

Active Information Gathering - Nmap

Mapping

NMAP: Most powerful and preferred port scanner for security professionals.

Scan Option	Name	Notes	Example
-sS	TCP SYN	Stealth scan. The full TCP connection is not established	#nmap –sS 192.168.1.0/24
-sT	TCP Full	Full connect. Most detectable	#nmap –sT 192.168.1.0/24
-sU	UDP	UDP scanning	#nmap –sU 192.168.1.0/24
-sP	Ping	Performs a ping sweep	#nmap –sP 192.168.1.0/24
-P0	Don't ping	Perform the scan even the target doesn't not respond to ping	#nmap –P0 192.168.1.0/24
-T<0-5>	Time	Set the timing template (higher is faster)	#nmap –O –T5 192.168.1.0/24
-p0-65535	TCP scan	It will scan all the 65,536 ports	#nmap –sS –p0-65535 192.168.1.1
-p22	Port	Port specification	#nmap –O –p22 192.168.1.1

Active Information Gathering – Nmap

Mapping

NMAP: Most powerful and preferred port scanner for security professionals.

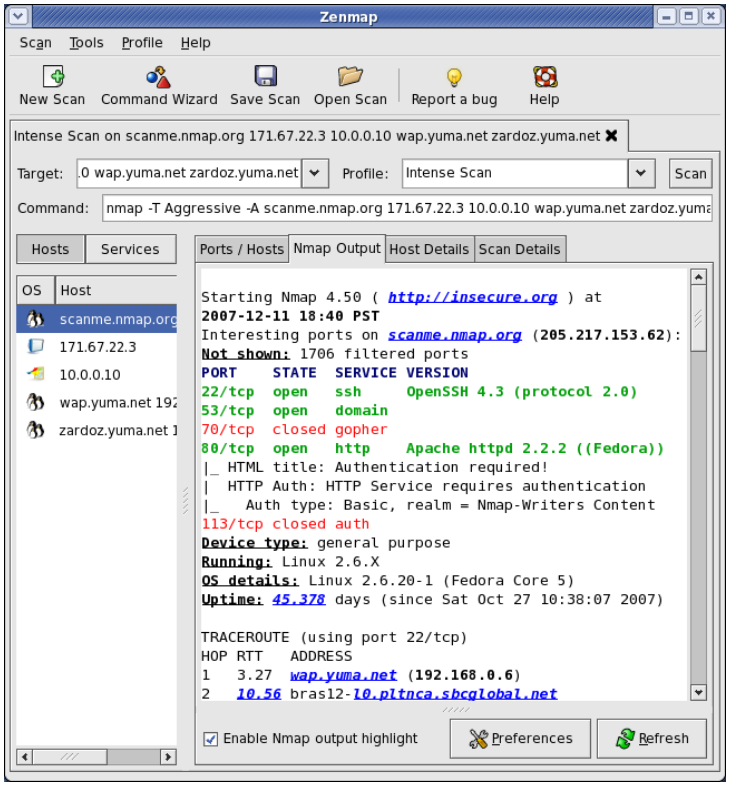
Scan Option	Name	Notes	Example
-sS	TCP SYN	Stealth scan. Called half opened scan because it never completes a connection with the target.	#nmap –sS 192.168.1.0/24
-sV	Service	Service detection	#nmap –sV –O 192.168.1.1
-O	OS Fingerprinting	It will try to find the OS running on the machine	#nmap –O 192.168.1.1
-sA	ACK scan	Shows which port is filtered or unfiltered by the Firewall	#nmap –sA 10.2.2.1
-D	Decoy	Shows that the scan attempt is coming from different sources.	#nmap –sS 10.2.2.1 –D 192.168.10.1,192.168.10.2,192.168.10.3
-sN	Null Scan	They are probes made with packets that violate traditional TCP connection.	#nmap –sN 10.2.2.1

Active Information Gathering – Zenmap

Mapping

ZENMAP: it is a graphical interface of Nmap.

- Can do a comparison between scans;
- Keeps track of the scan results;
- It can even draw a topological map of the discovered network.



> Backtrack | Information Gathering | Network Analysis | Identify Live Hosts

Project – Phase 1: Recon & Mapping

Reconnaissance

Goal

- **Step 1:** Gathering information;
- **Step 2:** Locating the network range;
- **Step 3:** Identifying active machines;
- **Step 4:** Finding open ports and applications;
- **Step 5:** Detecting operating systems;
- **Step 6:** Fingerprinting services;
- **Step 7:** Mapping the network.

Project – Phase 1: Recon & Mapping

Reconnaissance & Mapping

- Please use the tools just presented to provide as much of information as possible to your report;
- List the IP ranges, the services used by each host, DNS names, domain;
- Please use at least 3 different tools to check the service version;
- Focus on ports: TCP 80, 808X, 800X, 8180, 443.

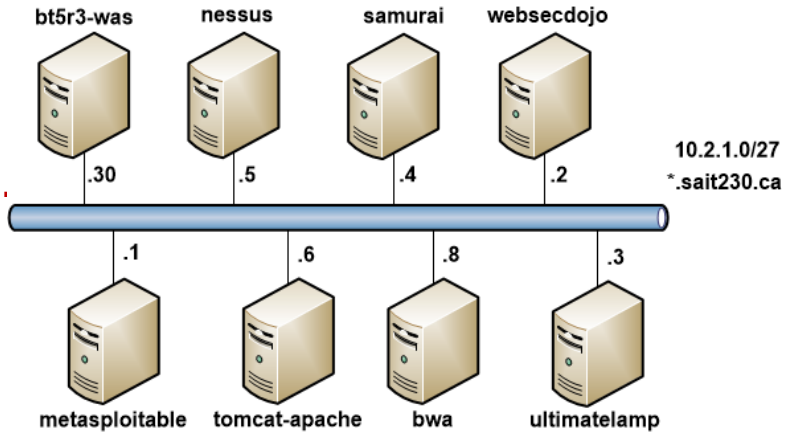
Example

Company Name: Sait230 INC.

Domain Names: sait230.ca, sait230.

IP ranges: 10.X.X.X/??

Logical Topology



Project – Phase 1: Recon & Mapping

Reconnaissance & Mapping

Hostname	IP	Service	Version	Port

Project – Phase 1: Recon & Mapping

Reconnaissance & Mapping

Hostname	IP	Service	Version	Port

Questions