NYU TANDON SCHOOL OF ENGINEERING

Network Security

CS6823 – Lesson 2
Network Reconnaissance

Phillip Mak
pmak@nyu.edu

Exploiting Systems – Why Teach?

- Much controversy over teaching “how to hack”
- Why should we learn this?
- You have to know how networks are attacked in order mount an effective defense.
- “Know your enemy”
- However, with this knowledge comes responsibility.
- Much like if you learn how to fire a weapon you only do it at the pistol range not in the middle of the street.
- *Likewise, skills taught here are to only be used in the confines of a controlled computer security research lab.*
- *If you go out and do something stupid – you will end up in jail.*

Some Additional Words of Caution

- General Assumption = Bypassing a protection is illegal
- Penetration testing is bypassing protections with explicit written PERMISSION from the owner of the system.
- However, in Germany and France and some other EMEA countries place the development or possession of “attack” tools as illegal.
- Legal advice is critical (this slide is not legal advice)

Lesson Objectives

- Understand the six steps of the Network Reconnaissance
- Enumerate and describe methods, both technical and non-technical, to collect information from public sources
- Understand and apply whois and DNS Reconnaissance methods, including how DNS works (DNS Zone Transfers and DNS Brute Forcing, and Split DNS)
- Understand the fields in a IP, TCP, UDP, and ICMP header
- Describe the method and possible responses for port scanning with TCP and UDP packets
- Describe all nmap scan types, purposes, and advantages and disadvantages of each type

Types of Attacks and Computer Crimes

- Denial of Service
- Destruction of Information
- Dumpster Diving
- Emanation
- Eavesdropping
- Embezzlement
- Espionage
- Fraud
- Information Warfare
- Illegal Content or Material
- Malicious Code
- Masquerading
- Social Engineering
- Software Piracy
- IP Address Spoofing
- Terrorism
- Theft of Passwords
- Use of exploit scripts
- Network Intrusions

See notes section for definitions

Why?

Fame

Not so much anymore (more on this with Trends)

Money

The root of all evil…

War

A battlefront just as real as the air, land, and sea

Mar 20, 2013 - The computer networks of three major South Korean banks and three television networks went offline nearly simultaneously at 2pm Seoul time on Wednesday, according to South Korea's National Police Agency. The government confirmed that malware was used to bring the networks down, and it is looking into whether North Korea is behind the attack.

US Federal Computer Crime Laws (consult legal council for official advice)

Note: The following slides on laws is to facilitate discussion only. There is no need to memorize any of these details. Will not be tested.

- 1970 US Fair Credit Reporting Act (FCRA) – Regulates the collection, dissemination and use of consumer credit information, amended several times
- 1970 US Racketeer Influenced and Corrupt Organization Act (RICO) – extends criminal and civil penalties for acts performed as part of a criminal organization
- 1973 Code of Fair Information Practices. Five underlying principals:
  1. No personal data recordkeeping systems whose existence is secret. (transparency)
  2. Must be a way for a person to find out what information about them is in a record and how it is used. (individual participation)
  3. There must be a way for a person to prevent information obtained for a specific purpose from being used for another purpose without the subjects consent. (purpose limitation)
  4. There must be a way for a person to correct a record of information about them. (integrity)
  5. Any organization creating, maintaining, using or disseminating records of personal data must assure the reliability of the data and take prudent measures to protect this data. (integrity)

US Federal Laws (cont)

- 1974 US Privacy Act – Who is allowed to have access to information that contains identifying info (education, criminal, medical records – but no limited to)
- 1978 Foreign Intelligence Surveillance Act (FISA) – Covers electronic surveillance of foreign intelligence organizations.
- 1986 US Computer Fraud and Abuse Act (amended in 1996) – covers malicious threats, attacks and unauthorized access to computer systems. Penalties increases with Patriot Act.1987
- 1994 US Communications Assistance for Law Enforcement Act – This law requires all communications carriers to provide a facility for law enforcement to provide wiretaps.

US Federal Laws (cont)

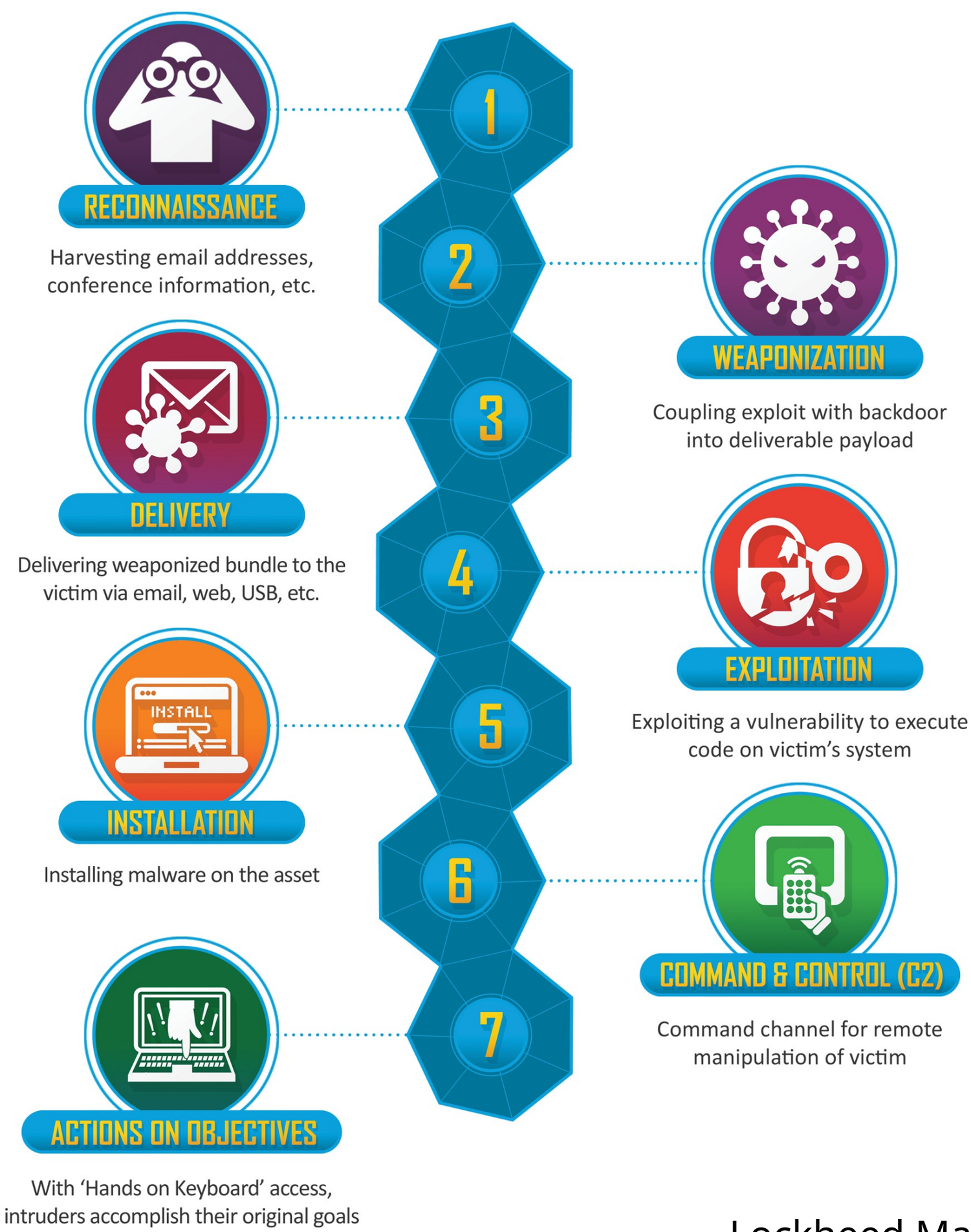
- 1996 Health Insurance and Portability Accountability Act (HIPPA – Amended in 2000) - Protecting personal information in the health insurance industry.
- 1996 Title 1, Economic Espionage Act – Make theft of trade secrets a crime
- 1998 US Digital Millennium Copyright Act (DMCA) – prohibits the manufacturing, trading or selling of any technology, device or service design to circumvent copy protection mechanisms

US Federal Laws (cont)

- US Uniform Computers Information Transactions Act (UCITA) – covers software licensing, online access and other transaction between computer systems. Validates “shrink wrapped licensing”
- 2000 US Congress Electronic Signatures in Global and National Commerce Act (ESIGN) – legal foundation for electronic signatures and records
- 2001 USA Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act – Extends the ability of law enforcement to search electronic records.
- 2002 E-Govt Act Federal Information Security Management Act (FISMA) – improve security of computer networks in the federal government.

NYU | TANDON SCI OF ENGINEE

Cyber Kill Chai



Lockheed Martin

NYU TANDON SCHOOL OF ENGINEERING

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	BITS Jobs	Build Image on Host	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Escape to Host	Domain Policy Modification (2)	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Event Triggered Execution (16)	Execution Guardrails (1)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (3)	Implant Internal Image	Process Injection (12)	Hide Artifacts (10)	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (7)	Scheduled Task/Job (5)	Hijack Execution Flow (12)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)	Valid Accounts (4)	Impair Defenses (9)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal (9)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Input Capture (4)	Traffic Signaling (2)		
				Scheduled		Indirect Command Execution		Password Policy Discovery		Screen Capture	Web Service (3)		
						Masquerading (7)		Peripheral Device Discovery		Video Capture			
						Modify Authentication Process (7)		Permission Groups Discovery (3)					
						Modify Cloud Compute		Process Discovery					
								Query Registry					

RECONNAISSANCE - INFORMATION GATHERING

Harvesting email addresses, conference information, etc.

Reconnaissance

- “Casing the joint”
- Gather as much information as possible about the target from open sources
- Bank robbers will typically perform reconnaissance on the branch. Will observe times when the branch is busy with customers, guard shift changes, location of cameras, etc.
- This is the same first step performed in computer network attacks.

What are we trying to get?

- IP addresses
- Network Topology
- Domain Names
- User Account Names
- Operating systems and software being used
- Security Policies: password complexity requirements, change policy
- Physical security systems
- Home addresses of employees
- Frequent hangouts of employees
- And more

1- Collect Public Information

Collecting Information from Public Sources

- Public Information Sources
  Public Databases

- Dumpster Diving
  Shred your documents

- Social Engineering
  Educate your users about giving out sensitive or confidential information over the phone. Caller-id DOES NOT provide authentication

- Domain name system (DNS) or searching services (i.e., traceroute.com)

- Physical Break Ins
  You can have the best, multimillion dollar security system on the market but it will be useless if you don't lock the front door.

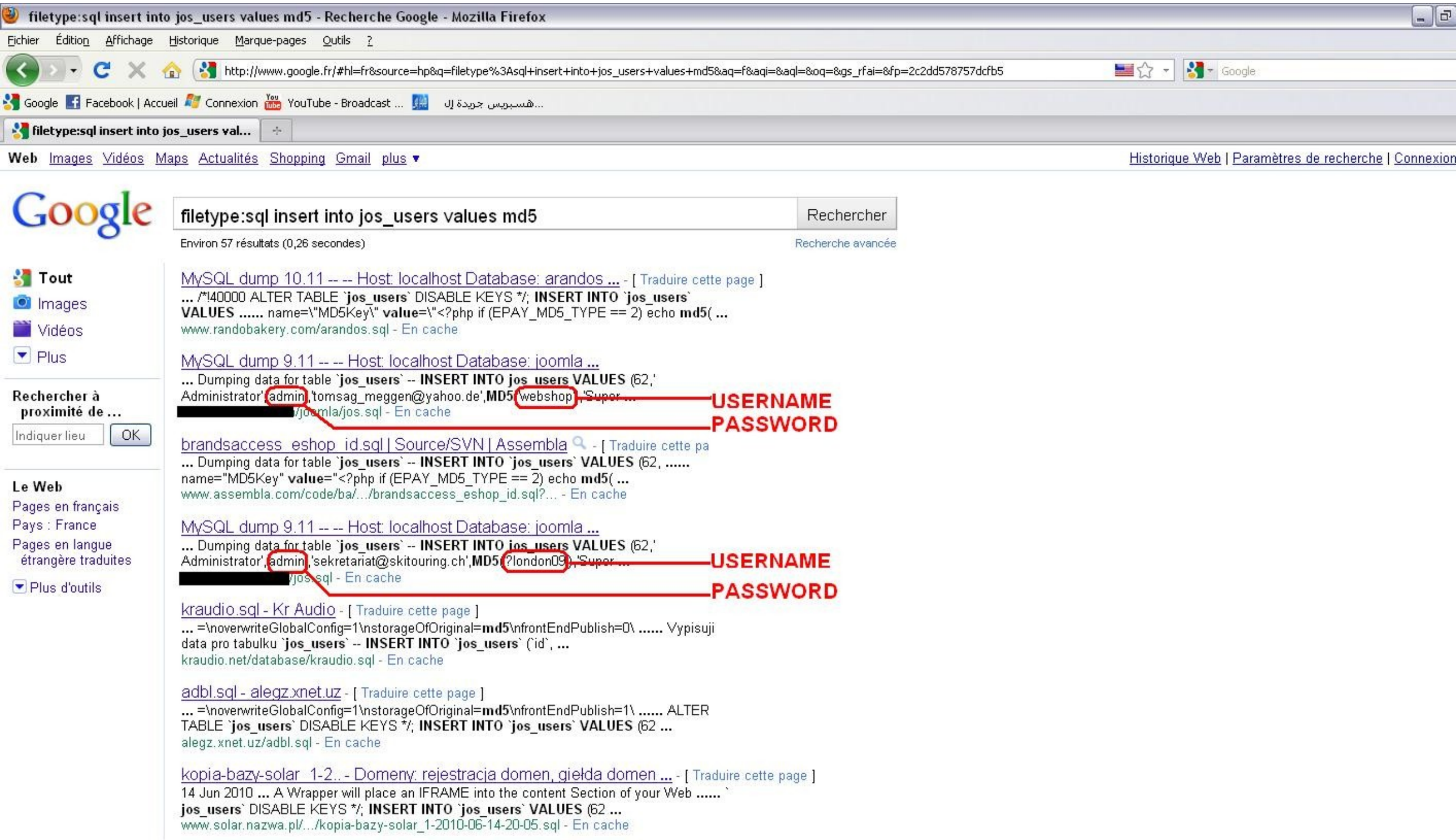
Changing Caller-ID is Easy

- There are legitimate reasons to do this.
  For example, I work from home often. When I call business associates from home I would like my "work" number displayed.
- Has been around for a long time but used to require dedicated PRI lines and expensive equipment
- Now can setup Asterisk server (free and open source) and signup for a very low cost VoIP trunking provider. Just need a spare PC and broadband connection.
- Or even easier:

Useful Google Searches

- “site:” directive – searches only within a given domain site:poly.edu
- “intitle:” – shows pages whose title matches the search criteria.
- “inurl:” – shows pages whose URL matches the search string
- “related:” – shows similar pages.

Google search of: `filetype:sql "insert into jos_users values" md5`



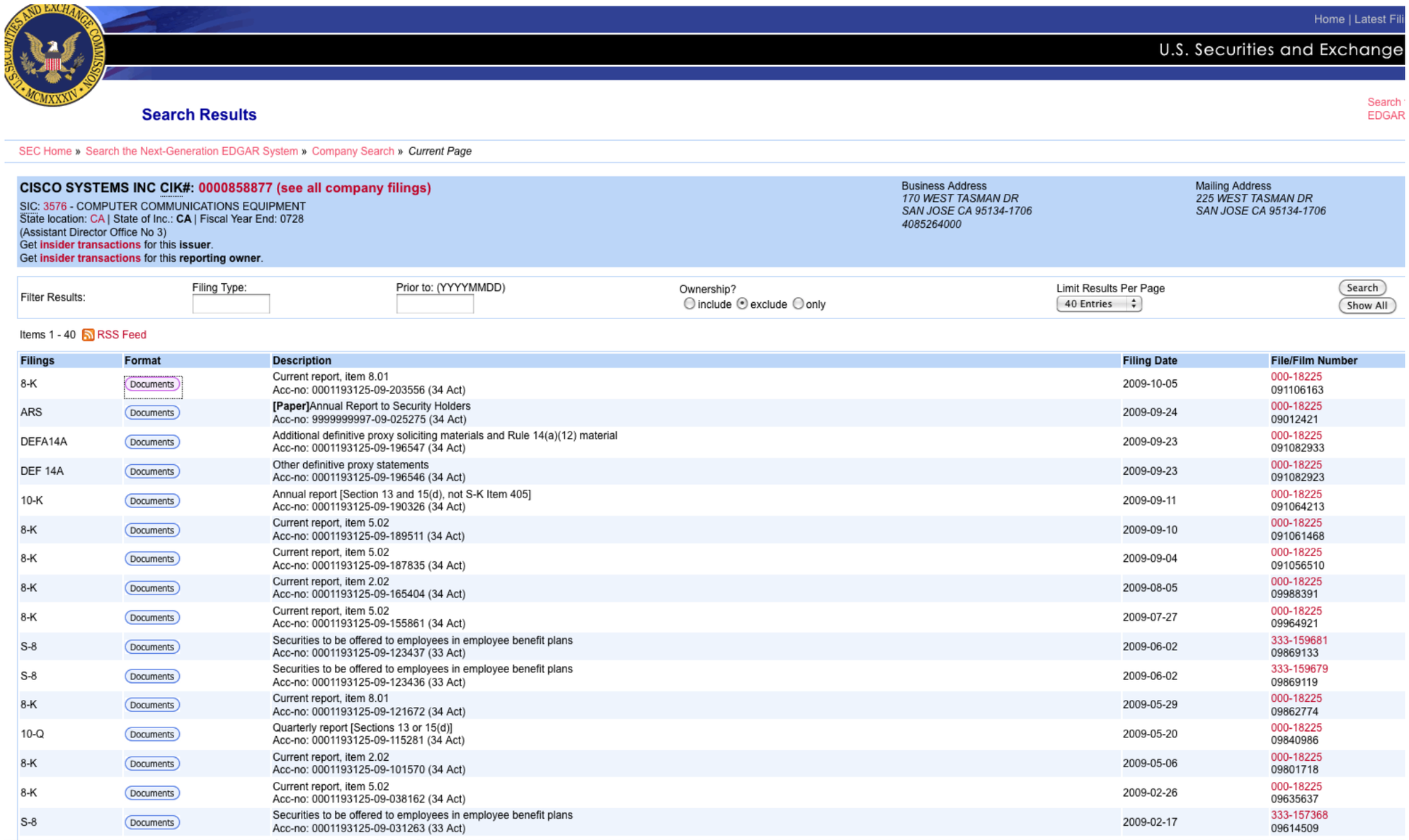
Google Recon Automated

- Performing reconnaissance using google can be easily automated with known searches

- Google Hacking Database (https://www.exploit-db.com/google-hacking-database)

Edgar Database – www.sec.gov

If the company is public traded the Edgar database can be a valuable resource



Home | Latest Fili

U.S. Securities and Exchange

Search
EDGAR

Search Results

SEC Home » Search the Next-Generation EDGAR System » Company Search » *Current Page*

CISCO SYSTEMS INC CIK#: 0000858877 (see all company filings)
SIC: 3576 - COMPUTER COMMUNICATIONS EQUIPMENT
State location: CA | State of Inc.: **CA** | Fiscal Year End: 0728
(Assistant Director Office No 3)

Business Address
170 WEST TASMAN DR
SAN JOSE CA 95134-1706
4085264000

Mailing Address
225 WEST TASMAN DR
SAN JOSE CA 95134-1706

Get **insider transactions** for this **issuer**.
Get **insider transactions** for this **reporting owner**.

Filter Results: | Filing Type: | Prior to: (YYYYMMDD) | Ownership? include / exclude / only | Limit Results Per Page: 40 Entries | Search | Show All

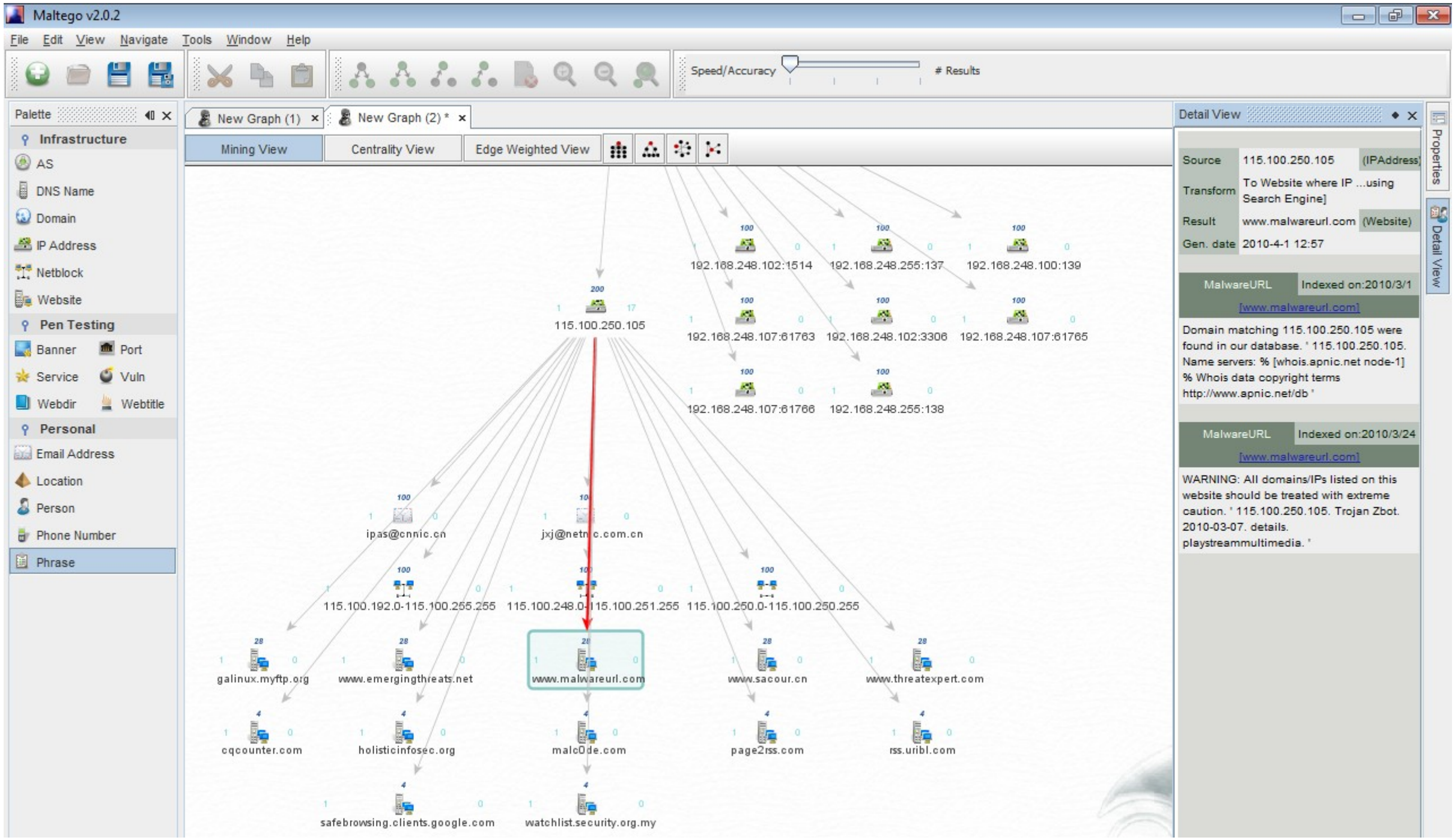
Items 1 - 40 RSS Feed

Filings	Format	Description	Filing Date	File/Film Number
8-K	Documents	Current report, item 8.01 Acc-no: 0001193125-09-203556 (34 Act)	2009-10-05	000-18225 091106163
ARS	Documents	**[Paper]**Annual Report to Security Holders Acc-no: 9999999997-09-025275 (34 Act)	2009-09-24	000-18225 09012421
DEFA14A	Documents	Additional definitive proxy soliciting materials and Rule 14(a)(12) material Acc-no: 0001193125-09-196547 (34 Act)	2009-09-23	000-18225 091082933
DEF 14A	Documents	Other definitive proxy statements Acc-no: 0001193125-09-196546 (34 Act)	2009-09-23	000-18225 091082923
10-K	Documents	Annual report [Section 13 and 15(d), not S-K Item 405] Acc-no: 0001193125-09-190326 (34 Act)	2009-09-11	000-18225 091064213
8-K	Documents	Current report, item 5.02 Acc-no: 0001193125-09-189511 (34 Act)	2009-09-10	000-18225 091061468
8-K	Documents	Current report, item 5.02 Acc-no: 0001193125-09-187835 (34 Act)	2009-09-04	000-18225 091056510
8-K	Documents	Current report, item 2.02 Acc-no: 0001193125-09-165404 (34 Act)	2009-08-05	000-18225 09988391
8-K	Documents	Current report, item 5.02 Acc-no: 0001193125-09-155861 (34 Act)	2009-07-27	000-18225 09964921
S-8	Documents	Securities to be offered to employees in employee benefit plans Acc-no: 0001193125-09-123437 (33 Act)	2009-06-02	333-159681 09869133
S-8	Documents	Securities to be offered to employees in employee benefit plans Acc-no: 0001193125-09-123436 (33 Act)	2009-06-02	333-159679 09869119
8-K	Documents	Current report, item 8.01 Acc-no: 0001193125-09-121672 (34 Act)	2009-05-29	000-18225 09862774
10-Q	Documents	Quarterly report [Sections 13 or 15(d)] Acc-no: 0001193125-09-115281 (34 Act)	2009-05-20	000-18225 09840986
8-K	Documents	Current report, item 2.02 Acc-no: 0001193125-09-101570 (34 Act)	2009-05-06	000-18225 09801718
8-K	Documents	Current report, item 5.02 Acc-no: 0001193125-09-038162 (34 Act)	2009-02-26	000-18225 09635637
S-8	Documents	Securities to be offered to employees in employee benefit plans Acc-no: 0001193125-09-031263 (33 Act)	2009-02-17	333-157368 09614509

Maltego

- Information gathering tool which visually displays the relationship between information.
  - Domain Names
  - Whois Information
  - DNS Names
  - Netblocks
  - IP Addresses
- Also allow for the enumeration of people
  - Email addresses
  - Web sites associated with a person
  - Phone numbers associated with a person's name
  - Social groups that are associated with a person
  - Companies and organizations associated with a person

Maltego

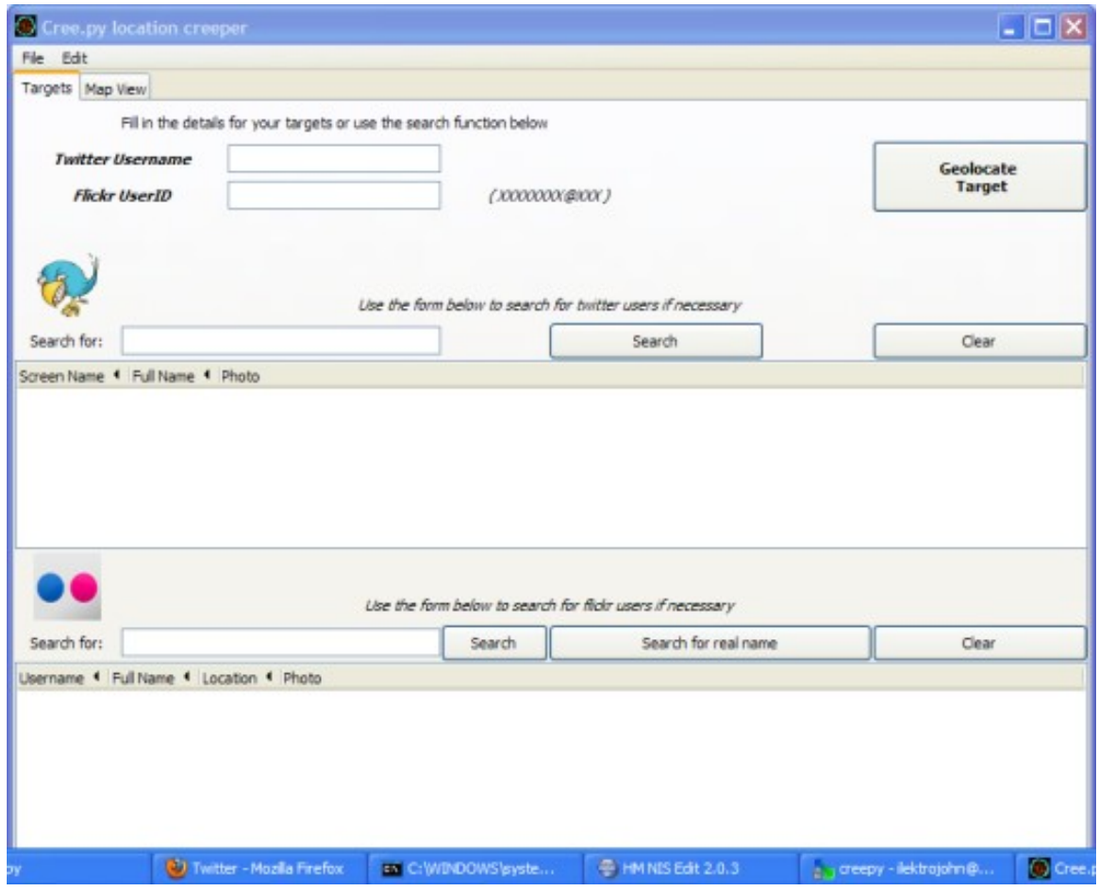

Maltego v2.0.2
File Edit View Navigate Tools Window Help
Speed/Accuracy
Results
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
New Graph (1)
New Graph (2) *
Mining View
Centrality View
Edge Weighted View
115.100.250.105
192.168.248.102:1514
192.168.248.255:137
192.168.248.100:139
192.168.248.107:61763
192.168.248.102:3306
192.168.248.107:61765
192.168.248.107:61766
192.168.248.255:138
ipas@cnnic.cn
115.100.192.0-115.100.255.255
115.100.248.0-115.100.251.255
115.100.250.0-115.100.250.255
galinux.myftp.org
www.emergingthreats.net
www.malwareurl.com
www.sacour.cn
www.threatexpert.com
cqcounter.com
holisticinfosec.org
malc0de.com
page2rss.com
rss.uribl.com
safebrowsing.clients.google.com
watchlist.security.org.my
Detail View
Source 115.100.250.105 (IPAddress)
Transform To Website where IP ...using Search Engine]
Result www.malwareurl.com (Website)
Gen. date 2010-4-1 12:57
MalwareURL Indexed on:2010/3/1
[www.malwareurl.com]
Domain matching 115.100.250.105 were found in our database. ' 115.100.250.105. Name servers: % [whois.apnic.net node-1] % Whois data copyright terms http://www.apnic.net/db '
MalwareURL Indexed on:2010/3/24
[www.malwareurl.com]
WARNING: All domains/IPs listed on this website should be treated with extreme caution. ' 115.100.250.105. Trojan Zbot. 2010-03-07. details. playstreammultimedia. '
Properties
Detail View

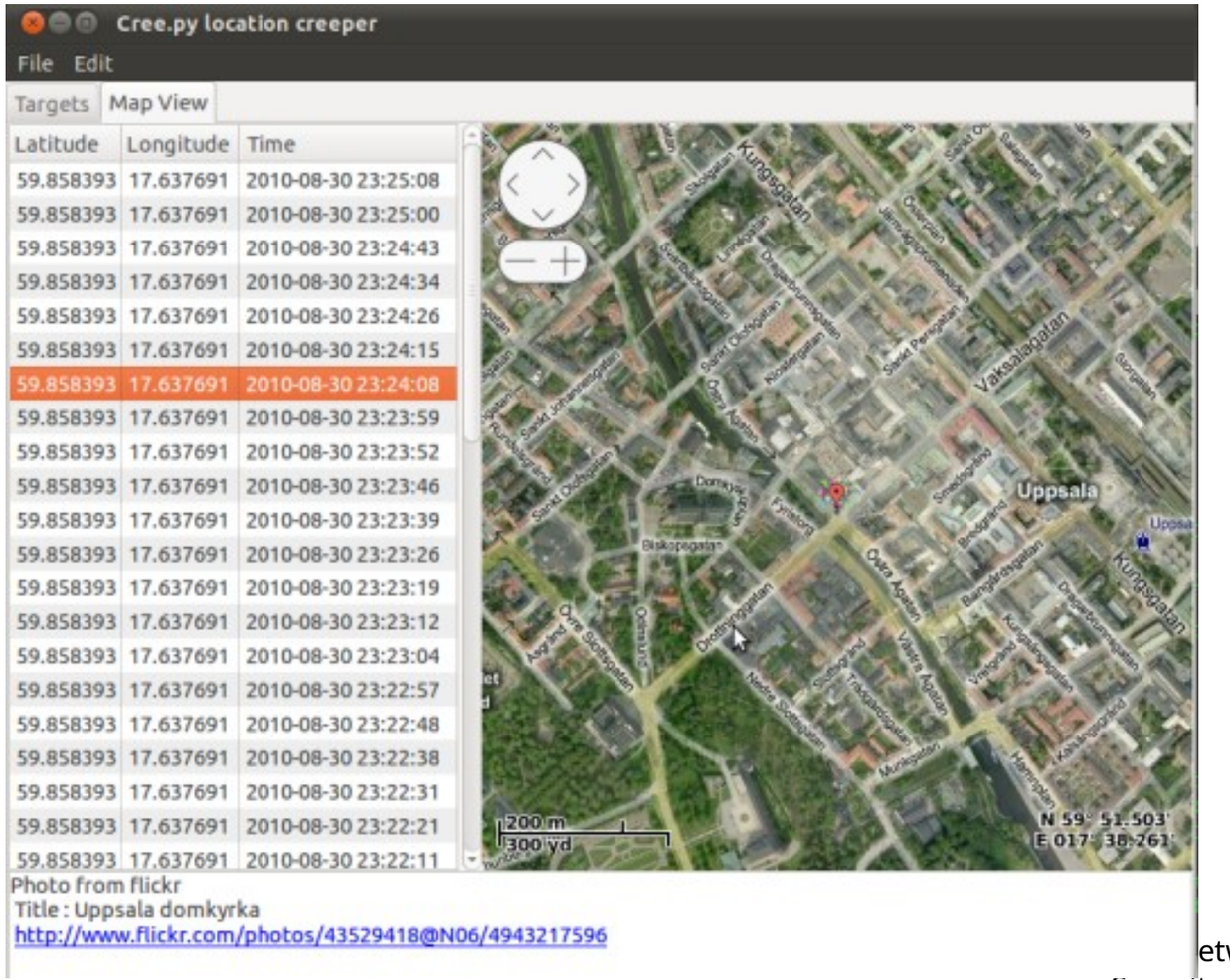
Individual – Social Network Profile

- Metadata Leakage
- Tone
- Frequency
- Location Awareness
- Social Media Presense

- Cree.py is an open source intelligence gathering application.

- Can gather from Twitter.





- Cree.py can gather any geo-location data from flickr, twitpic.com, yfrog.com, img.ly, plixi.com, twitrpix.com, foleext.com, shozu.com, pickhur.com, moby.to, twitsnaps.com and twitgoo.com.

NYU TANDON SCHOOL OF ENGINEERING

2 - Determine the Network Range (Scanning and Enumeration)

Whois Database

- Many website and domain registrars offer this service through the web.
- Can also use the built in “whois” command on many Unix systems.
- First looks up the target in InterNIC to determine the registrar: http://www.internic.net/whois.html
- Then go to the registrar for detailed records:
  - Ex. http://www.networksolutions.com/whois/index.jsp

DNS is a Treasure Trove of Info

- When you register a domain name with an authorized registrar you must provide a valid name, address and phone number of the person responsible for the domain.
- This information can be used against you in an attack

Also Get Registered IP Blocks

- Based on geographical location:
  - ARIN (American Registry for Internet Numbers)
    - www.arin.net (https://ws.arin.net/whois/)
  - RIPE (Reseaux IP Europeans Network Coordination Centre)
    - www.ripe.net
  - APNIC (Asia Pacific Network Information Center)
    - www.apnic.net
  - LACNIC (Latin American and Caribbean NIC)
    - www.lacnic.net
  - AFRINIC (Africa's NIC)
    - www.afrinic.net
  - DoDNIC (Department of Defense NIC)
    - www.nic.mil - not open to the outside
  - Other useful sites:
    - www.allwhois.com www.uwhois.com

Poly.edu WHOIS Reconnaissance

```
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.net

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail. The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

You may use "%" as a wildcard in your search. For further
information regarding the use of this WHOIS server, please
type: help

--------------------------

Domain Name: POLY.EDU

Registrant:
Polytechnic University
6 Metrotech Center
Brooklyn, NY 11201
UNITED STATES

Administrative Contact:
Information Systems Department Polytechnic University
Polytechnic University
6 Metrotech Center
Brooklyn, NY 11201
UNITED STATES
(718) 260-3573
network@poly.edu

Technical Contact:
Information Systems Department Polytechnic University
Polytechnic University
6 Metrotech Center
Brooklyn, NY 11201
UNITED STATES
(718) 260-3573
network@poly.edu

Name Servers:
GATEKEEPER.POLY.EDU 128.238.2.38
PHOTON.POLY.EDU 128.238.32.22

Domain record activated: 24-Jan-1995
Domain record last updated: 05-Jun-2006
Domain expires: 31-Jul-2010
```

DNS Record Types

A	ADDRESS RECORD. DESCRIBES THE IP ADDRESS THAT A GIVEN NODE HAS
MX	MAIL EXCHANGE. IP ADDRESS OF THE SERVER WHICH HANDLES MAIL FOR THE DOMAIN
NS	NAME SERVER. DOMAIN NAME SERVERS WHICH SERVE THIS DOMAIN NAME
CNAME	CANONICAL NAME. ALIASES FOR HOST NAMES
SOA	FIRST LINE OF DNS FILE. INDICATES THAT THIS SERVER IS THE BEST SOURCE OF INFORMATION FOR THIS DOMAIN
SRV	SERVICE RECORD. INFORMATION ABOUT AVAILABLE SERVICE IN THE DOMAIN. SIP AND XMPP USE THIS.
RP	RESPONSIBLE PERSON. ASSIGN AN EMAIL ADDRESS TO A SPECIFIC HOST
PTR	POINTER RECORD. ALLOWS FOR REVERSE DNS LOOKUP. TYPICALLY REQUIRED FOR MX HOSTS
TXT	ORIGINALLY FOR HUMAN READABLE INFORMATION. BUT NOW USED FOR THINGS SUCH AS DOMAIN-KEYS
HINFO	HOST INFO. SUPPLIES OS AND OTHER INFO ABOUT A HOST. GENERALLY NOT A GOOD IDEA.

Polv.edu DNS Reconnaissance

DNS Records

base	record	name	ip	reverse	route	as
poly.edu 20 hours old	a		128.238.1.62 United States	poly-ad-vm-01.poly.edu	128.238.0.0/16 Proxy-registered route object	AS23329 OA631 Open Access Inc. (website: www.openaccessinc.com)
			128.238.1.63 United States	poly-ad-vm-02.poly.edu		
			128.238.1.68 United States	dns-vm-01.poly.edu		
			128.238.24.30 United States	(none)		
			128.238.24.40 United States			
			128.238.111.50 United States	poly-ad-dr-vm-01.poly.edu		
	ns	gatekeeper.poly.edu 268 days old	128.238.2.38 United States			
		photon.poly.edu 41 days old	128.238.32.22 United States			
	mx	20 mail.poly.edu 268 days old	128.238.2.92 United States	duke.poly.edu		
		2 poly.edu.s8a1.psmtp.com 5 days old	64.18.7.10 United States	s8a1.psmtp.com	64.18.7.0/24 LLNW cust	AS26910 Postini Network
		4 poly.edu.s8a2.psmtp.com 268 days old	64.18.7.11 United States	s8a2.psmtp.com		
		6 poly.edu.s8b1.psmtp.com 268 days old	64.18.7.13 United States	s8b1.psmtp.com		
		8 poly.edu.s8b2.psmtp.com 268 days old	64.18.7.14 United States	s8b2.psmtp.com		
		10 duke.poly.edu 20 hours old	128.238.2.92 United States		128.238.0.0/16 Proxy-registered route object	AS23329 OA631 Open Access Inc. (website: www.openaccessinc.com)
edu 2 hours old	ns	a.gtld-servers.net 17 hours old	192.5.6.30 United States		192.5.6.0/24 VeriSign Route	AS36621 VERISIGN-AS VeriSign, Inc
		c.gtld-servers.net 3 hours old	192.26.92.30 United States		192.26.92.0/24 VeriSign Route	AS36619 VERISIGN-AS VeriSign, Inc
		d.gtld-servers.net 6 hours old	192.31.80.30 United States		192.31.80.0/24 VeriSign Route	AS36617 VERISIGN-AS VeriSign, Inc
		e.gtld-servers.net 1 hour old	192.12.94.30 United States		192.12.94.0/24 VeriSign Route	AS36629 VERISIGN-AS VeriSign, Inc
		f.gtld-servers.net 8 hours old	192.35.51.30 United States		192.35.51.0/24 VeriSign Route	AS36620 VERISIGN-AS VeriSign, Inc
		g.gtld-servers.net 1 day old	192.42.93.30 United States		192.42.93.0/24 VeriSign Route	AS36624 VERISIGN-AS VeriSign, Inc
		l.gtld-servers.net 23 hours old	192.41.162.30 United States		192.41.162.0/24 VeriSign Route	AS36628 VERISIGN-AS VeriSign, Inc

net gtld-servers.net psmtp.com com edu.s8a2.psmtp.com edu.s8a1.psmtp.com edu.s8b1.psmtp.com edu.s8b2.psmtp.com

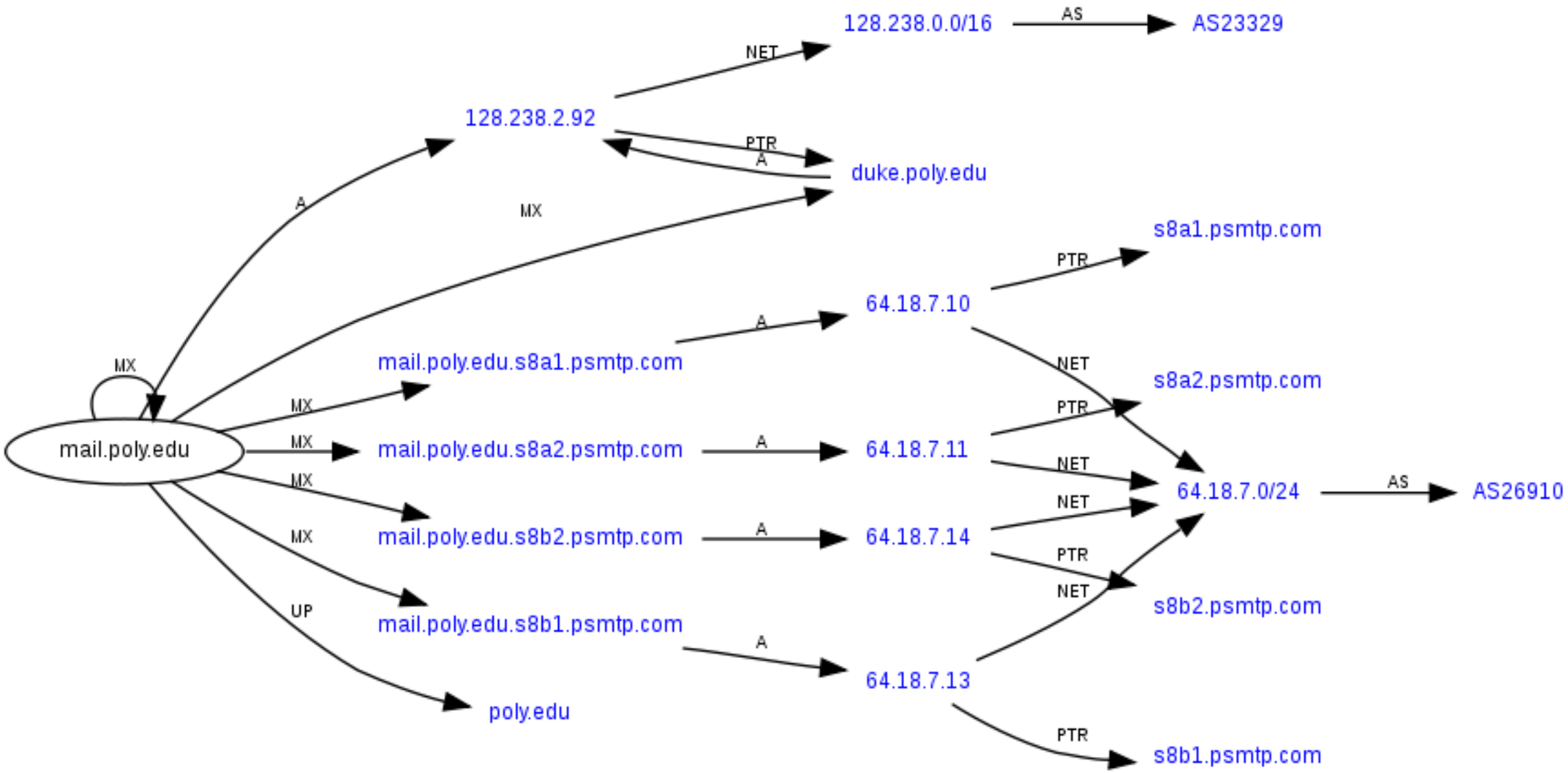
Lets dig into mail.poly.edu:

DNS Records

base	record	name	ip	reverse	route	as
mail.poly.edu	a		128.238.2.92 United States	duke.poly.edu	128.238.0.0/16 Proxy-registered route object	AS23329 OA631 Open Access Inc. (website: www.openaccessinc.com)
	mx 20	mail.poly.edu	128.238.2.92 United States	duke.poly.edu		
	2	mail.poly.edu.s8a1.psmtp.com 320 days old	64.18.7.10 United States	s8a1.psmtp.com	64.18.7.0/24 LLNW cust	AS26910 Postini Network
	4	mail.poly.edu.s8a2.psmtp.com 320 days old	64.18.7.11 United States	s8a2.psmtp.com		
	6	mail.poly.edu.s8b1.psmtp.com 320 days old	64.18.7.13 United States	s8b1.psmtp.com		
	8	mail.poly.edu.s8b2.psmtp.com 320 days old	64.18.7.14 United States	s8b2.psmtp.com		
	10	duke.poly.edu 20 hours old	128.238.2.92 United States		128.238.0.0/16 Proxy-registered route object	AS23329 OA631 Open Access Inc. (website: www.openaccessinc.com)
poly.edu 20 hours old	a		128.238.1.62 United States	(none)		
			128.238.1.63 United States			
			128.238.1.68 United States			
			128.238.24.30 United States			
			128.238.24.40 United States			
			128.238.111.50 United States			
	ns	gatekeeper.poly.edu 268 days old	128.238.2.38 United States			
		photon.poly.edu 41 days old	128.238.32.22 United States			
	mx 20	mail.poly.edu	128.238.2.92 United States	duke.poly.edu		
	2	poly.edu.s8a1.psmtp.com 5 days old	64.18.7.10 United States	s8a1.psmtp.com	64.18.7.0/24 LLNW cust	AS26910 Postini Network
	4	poly.edu.s8a2.psmtp.com 268 days old	64.18.7.11 United States	s8a2.psmtp.com		
	6	poly.edu.s8b1.psmtp.com 268 days old	64.18.7.13 United States	s8b1.psmtp.com		
	8	poly.edu.s8b2.psmtp.com 268 days old	64.18.7.14 United States	s8b2.psmtp.com		
	10	duke.poly.edu 20 hours old	128.238.2.92 United States		128.238.0.0/16 Proxy-registered route object	AS23329 OA631 Open Access Inc. (website: www.openaccessinc.com)

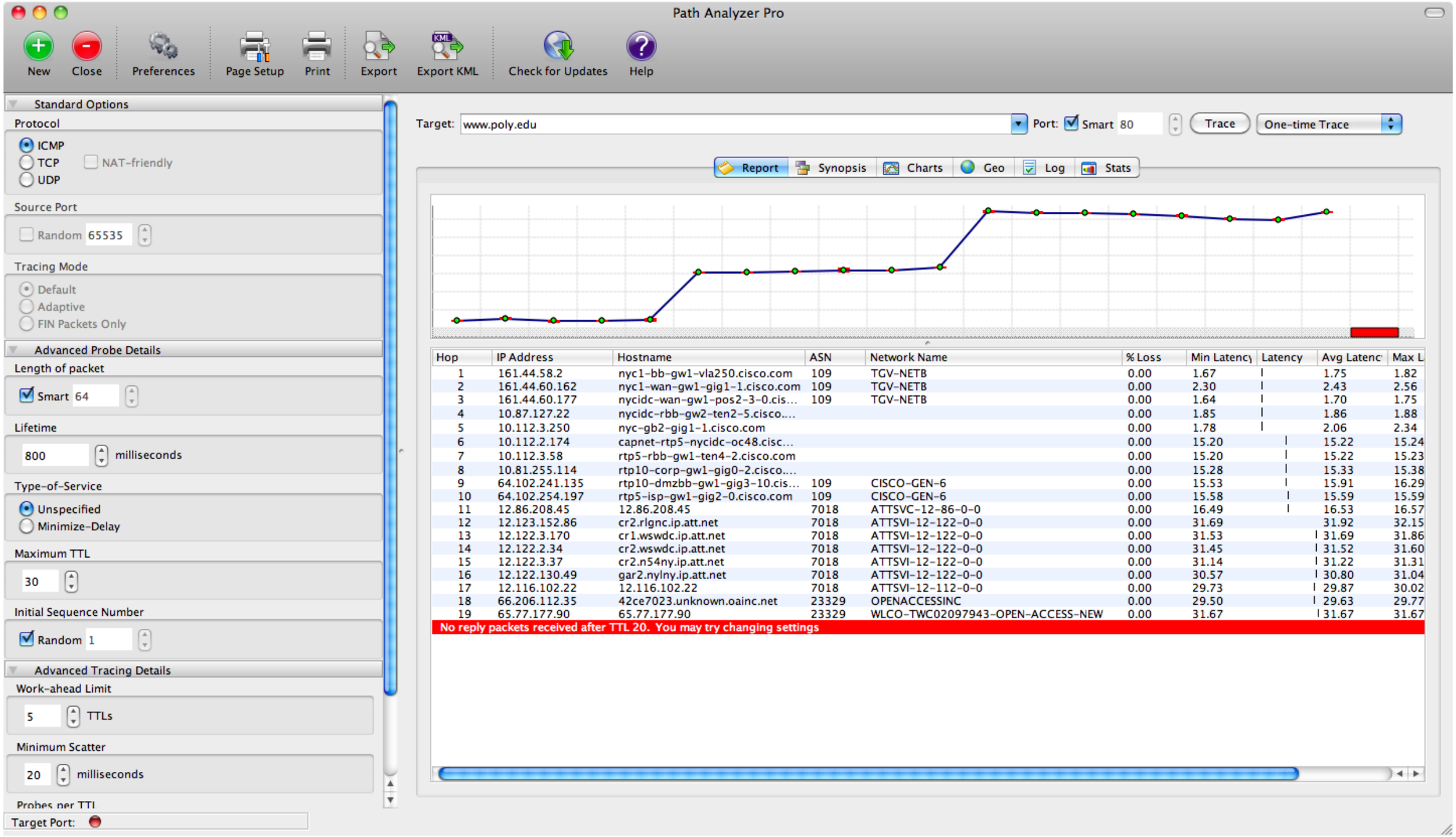
edu psmtp.com com edu.s8a2.psmtp.com edu.s8a1.psmtp.com edu.s8b1.psmtp.com edu.s8b2.psmtp.com

Map of mail.poly.edu



See: http://www.robtex.com

Gather Other Network Information



BGP “Looking Glass Servers”

```
home-macpro:~ kobrien$ telnet route-server.twtelecom.net
Trying 66.162.47.58...
Connected to route-server.twtelecom.net.
Escape character is '^]'.
C
**************************************************************************
**                       route-server.twtelecom.net                     **
**                      tw twtelecom IP Route Monitor                   **
**                                AS 4323                               **
**************************************************************************

  This route server maintains peering sessions with several border
routers within the tw telecom nation wide US network.

                168.215.52.101  Atlanta, GA
                168.215.52.9    Chicago, IL
                168.215.52.192  Denver, CO
                168.215.52.175  Los Angeles, CA
                168.215.52.70   New York, NY
                168.215.52.197  Oakland, CA
                168.215.52.203  Seattle, WA
```

BGP “Looking Glass Servers” (cont)

```
route-server>sh ip route 128.238.0.0
Routing entry for 128.238.0.0/16
  Known via "bgp 4323", distance 200, metric 0
  Tag 7018, type internal
  Last update from 168.215.52.202 5d10h ago
  Routing Descriptor Blocks:
  * 168.215.52.202, from 168.215.52.203, 5d10h ago
      Route metric is 0, traffic share count is 1
      AS Hops 2

route-server>tracert 128.238.2.92
                     ^
% Invalid input detected at '^' marker.

route-server>trace 128.238.2.92

Type escape sequence to abort.
Tracing the route to duke.poly.edu (128.238.2.92)

  1 ge-0-3-0-514.dnvr.twtelecom.net (66.162.47.57) 0 msec 0 msec 0 msec
  2 peer-01-so-1-0-0-0.dlfw.twtelecom.net (66.192.246.53) 16 msec 16 msec 16 msec
  3 cr2.dlstx.ip.att.net (12.122.138.18) [AS 7018] 52 msec 56 msec 52 msec
  4 cr1.attga.ip.att.net (12.122.28.173) [AS 7018] 56 msec 52 msec 56 msec
  5 cr2.wswdc.ip.att.net (12.122.1.174) [AS 7018] 56 msec 56 msec 56 msec
  6 cr2.n54ny.ip.att.net (12.122.3.37) [AS 7018] 56 msec 56 msec 56 msec
  7 gar2.nylny.ip.att.net (12.122.130.49) [AS 7018] 52 msec 56 msec 52 msec
  8 12.116.102.22 [AS 7018] 60 msec 56 msec 56 msec
  9 42ce7023.unknown.oainc.net (66.206.112.35) [AS 23329] 156 msec 56 msec 56 msec
 10 65.77.177.90 [AS 23329] 56 msec 56 msec 60 msec
 11 duke.poly.edu (128.238.2.92) [AS 23329] 60 msec 60 msec 60 msec
 12 duke.poly.edu (128.238.2.92) [AS 23329] 60 msec 60 msec 60 msec
```

Shodan

SHODAN ios 15.2 Search

Services

SNMP	918
SIP	6

Top Countries

United States	198
Italy	65
Netherlands	61
Russian Federation	60
France	59

Top Cities

Niteri	26
Brest	24
Kenmare	18
Moscow	11
Bangkok	10

Top Organizations

Global Village Telecom	28
SRT Telecomm	28
Level 3 Communications	21
TELECOM Bretagne	17
IX Networks BV io	16

83.69.76.12
CJSC Caucasus - Transtelekom
Added on 26.11.2012

Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9_NPE-M), Version 15.2(3)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 23-Mar-12 16:57 by prod_rel_team

200.179.206.65
Embratel
Added on 26.11.2012

Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(3)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Wed 13-Jun-12 14:24 by prod_rel_team

209.0.51.0
Level 3 Communications
Added on 26.11.2012

Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 20:54 by prod_rel_team

150.101.171.249
Internode Professional Access
Added on 26.11.2012
Perth

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

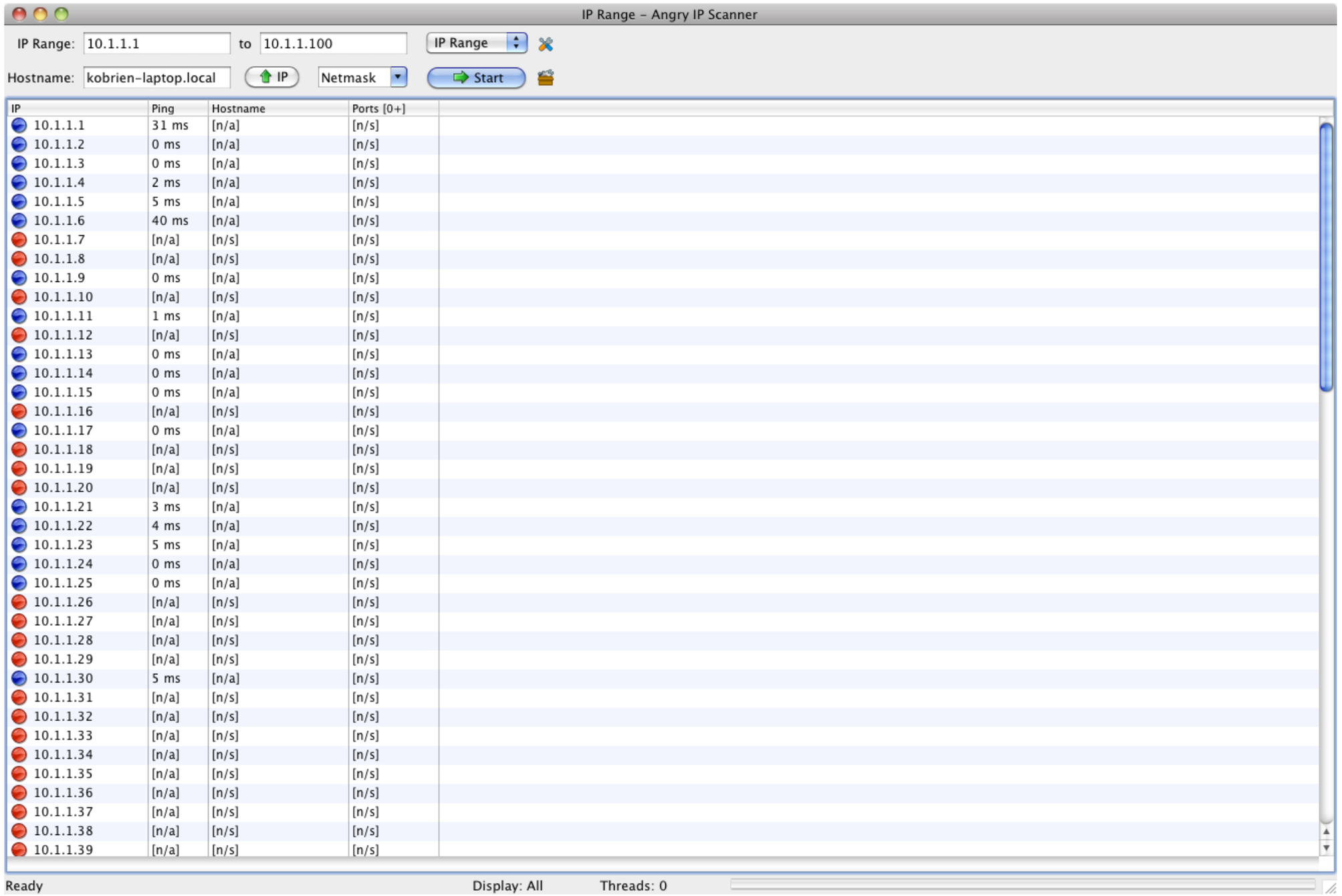
81.163.32.8
Subnet LLC
Added on 26.11.2012

Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-ADVIPSERVICES-M), Version 15.2(1)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.

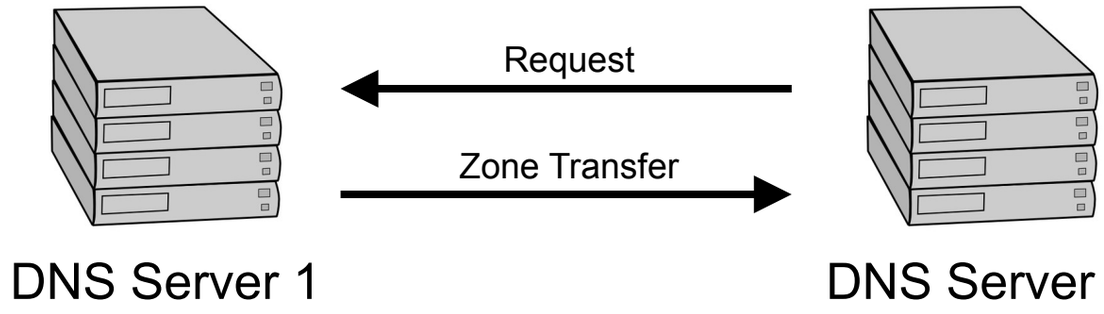
NYU TANDON SCHOOL OF ENGINEERING

3- Host Discovery

Ping Sweep – IP Scanner



DNS Zone Transfer

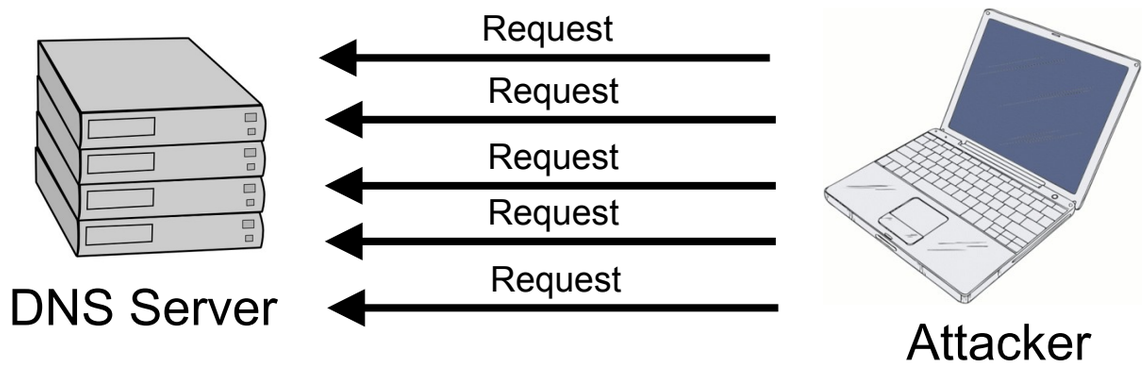


- On Linux systems dig can be used to perform a zone transfer from a DNS server.
- Very useful in recon and identifying targets.

dig @[DNS_server_IP] {target_domain] -t AXFR

```
kobrien@ubuntu-vm:~$ dig @10.1.1.3 example.org-t AXFR

; <<>> DiG 9.6.1-P2 <<>> @10.1.1.3 example.org -t AXFR
; (1 server found)
;; global options: +cmd
example.org.                    38400     IN        SOA       ns.example.org.example.org.
admin.example.org.example.org. 2008090354 10800 3600 604800 86400
example.org.                    38400     IN        NS        ns.example.org.
smtp.example.org.   38400     IN        CNAME     winserver.example.org.
switch.example.org. 38400     IN        A         10.1.1.2
linuxserv.example.org.          38400     IN        A         10.1.1.67
vmware.example.org. 38400     IN        A         10.1.1.25
winserver.example.org. 38400  IN        A         10.1.1.26
winserver-ca.example.org. 38400 IN      CNAME     winserver.example.org.
wireless.example.org. 38400   IN        A         10.1.1.14
example.org.                    38400     IN        SOA       ns.example.org.example.org.
admin.example.org.example.org. 2008090354 10800 3600 604800 86400
;; Query time: 18 msec
;; SERVER: 10.1.1.3#53(10.1.1.3)
;; WHEN: Tue Jan 26 10:55:54 2010
;; XFR size: 33 records (messages 1, bytes 840)
```

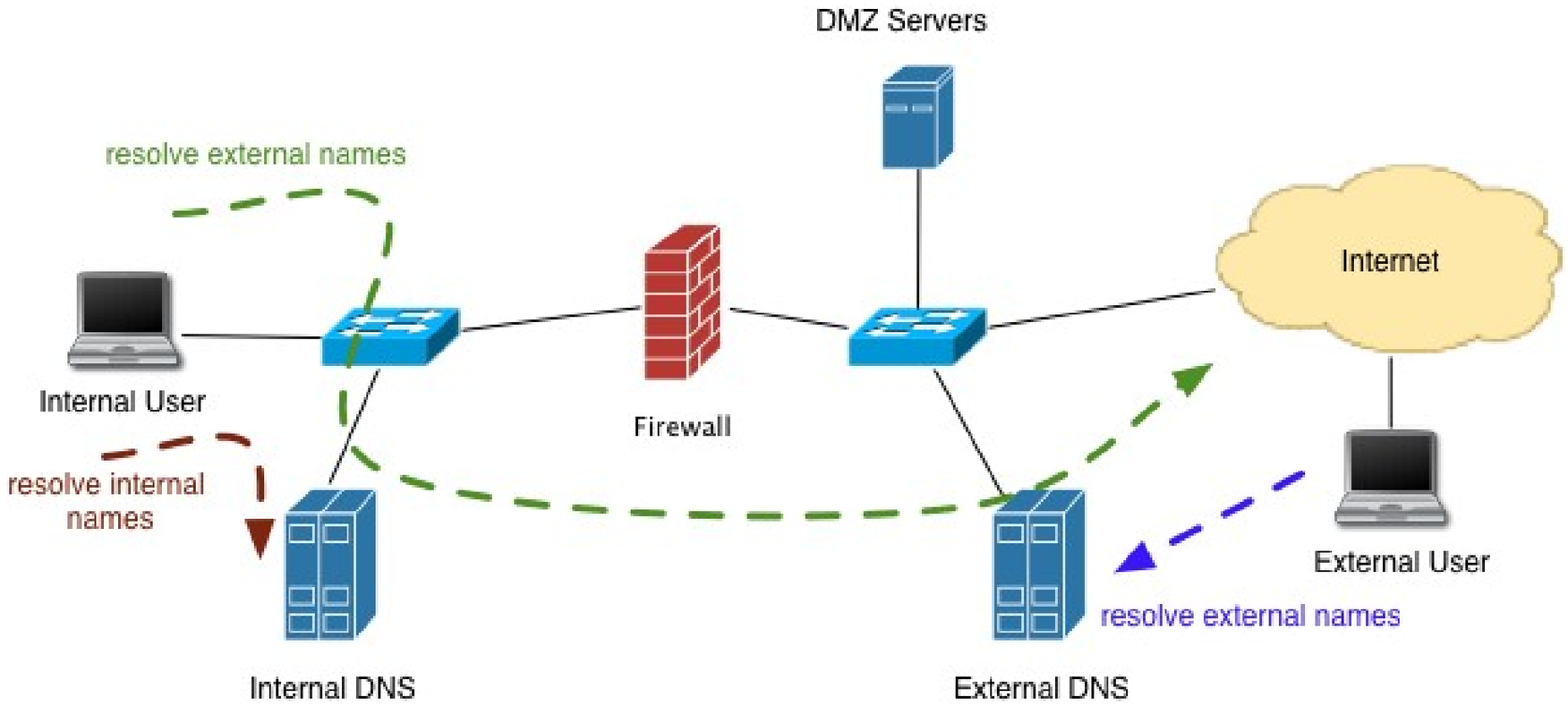
Brute Force Forward DNS




```
bt-netbook:/pentest/enumeration/dns/dnsmap# ./dnsmap example.org
dnsmap 0.22.2 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for obrienhome.org using built-in wordlist

firewall.example.org
IP address #1: 10.10.10.1

ftp.example.org
IP address #1: 10.10.10.3

ns.example.org
IP address #1: 10.10.10.3

smtp.example.org
IP address #1: 10.10.10.10

vpn.example.org
IP address #1: 10.10.10.1
```

Split DNS

External DNS has info on DMZ servers.
Internal DNS has info on internal servers.
Prevents leakage of internal DNS information



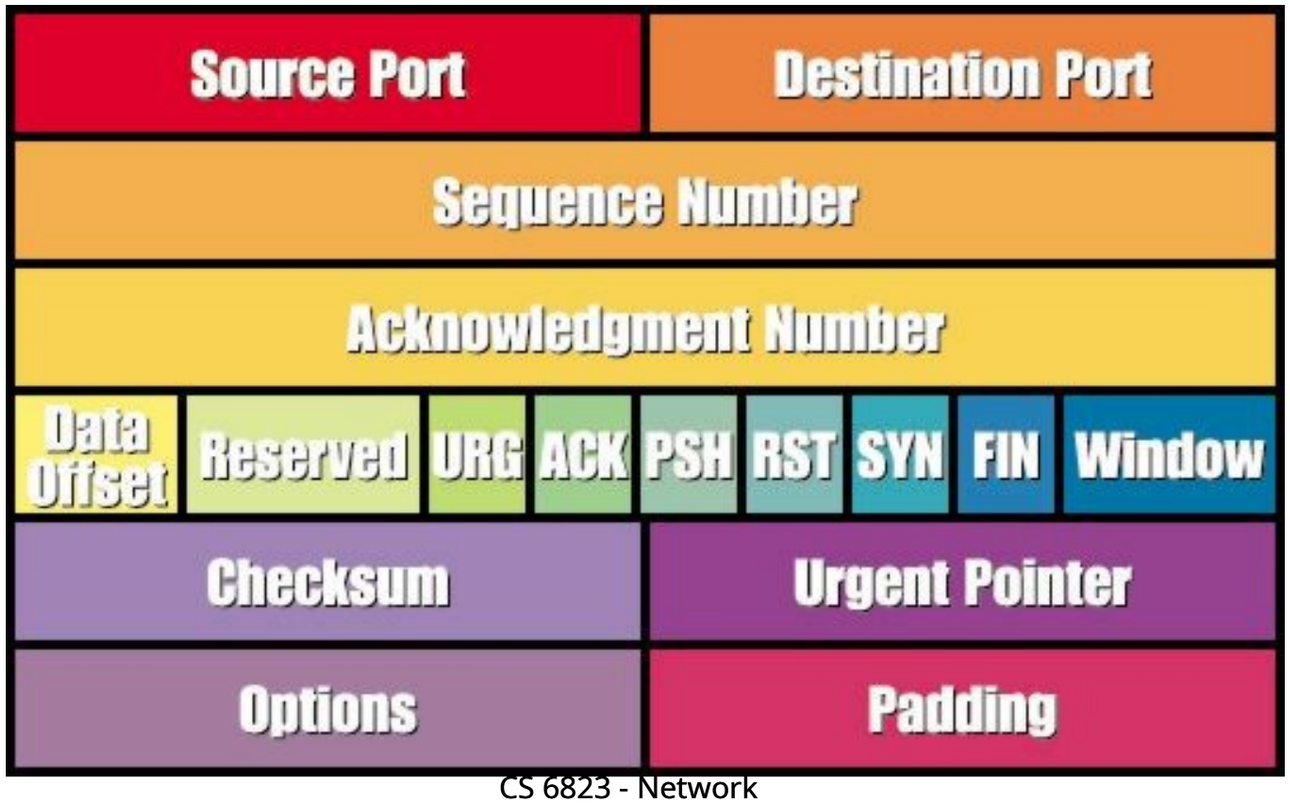
4 – Service Discovery

War Dialing

War dialers dial a sequence of phone numbers searching for modems or open PBXs
Modems are still prevalent for remote management of network equipment and infrastructure
Often they are left unprotected

TCP Control Bits

SYN – Synchronize
ACK – Acknowledgement
FIN – End a connection
RESET – Tear down a connection
URG – Urgent data is included
PUSH – Data should be pushed through the TCP stack

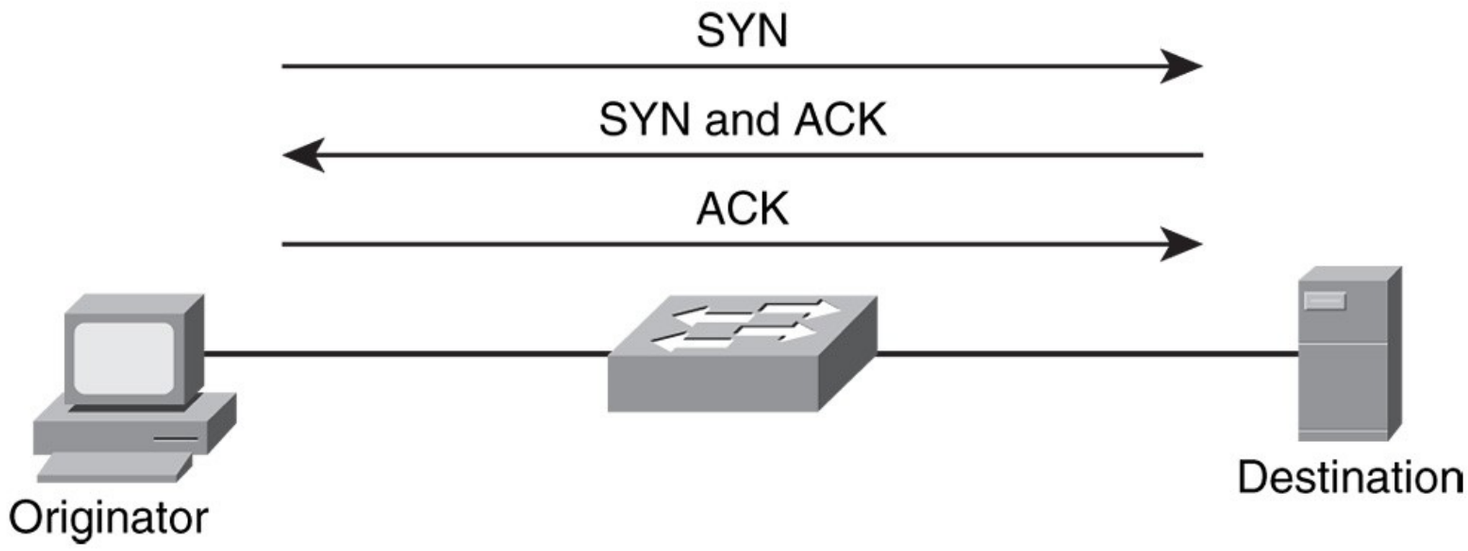


Port Scanning

Port scanners send TCP and UDP packets to various ports to determine if a process is active

- TCP 80 (web server)
- TCP 23 (telnet server)
- UDP 53 (DNS server)

TCP scanning based on 3 way handshake



HPING

Runs on all Unix-like systems. Also windows version.
Completely scriptable using TCL.
Can be used to write scripts implementing low level packet manipulation very quickly.

Example:

`hping3 -I en1 -S 10.1.1.1 -p 443` (sends packet to port 443 with SYN flag)

`Hping3 -l en1 -S 10.1.1.1 -p ++79` (sends packet with SYN flag. Increments by 1 starting at 79.)

HPING Switches (selected – see - - help)

```
-F --fin
-S --syn
-R --rst
-P --push
-A --ack
-U -urg
```

```
-s --baseport
-p -destport
-k --keep
-w --win
-O -tcpoff
-Q --seqnum
-b -badcksum
-M --setseq
-L --setack
```

HPING

Can also craft the payload of packets.
Useful for testing IPS/IDS systems.

```
# cat /root/signature.sig ""BUFFER OVERFLOW”

# hping -2 -p 7 10.1.1.1 -d 50 -E /root/signature.sig

HPING 192.168.10.33 (eth0 192.168.10.33): udp mode set, 28 headers + 50 data bytes
len=78 ip=192.168.10.33 seq=0 ttl=128 id=24842 rtt=4.9 ms
len=78 ip=192.168.10.33 seq=1 ttl=128 id=24844 rtt=1.6 ms
len=78 ip=192.168.10.33 seq=2 ttl=128 id=24846 rtt=1.0 ms
--- 192.168.10.33 hping statistic ---
3 packets tramitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.0/2.5/4.9 ms
```

NYU TANDON SCHOOL OF ENGINEERING

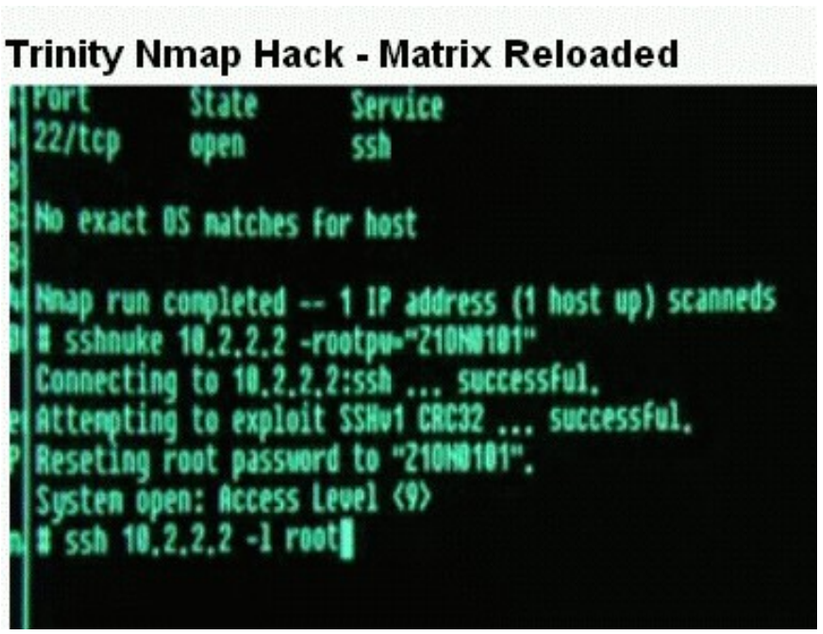
NMAP

Very popular port scanning tool

Written by “Fodor. http://insecure.org/nmap

Runs on Unix or Windows

GUI available (nmapfe)



NMAP – Scan Types

TCP Connect scan - This type of scan is the most reliable, although it is also the most detectable. It is easily logged and detected because a full connection is established. Open ports reply with a SYN/ACK, whereas closed ports respond with an RST/ACK. Uses standard connect() system call.

TCP SYN scan - This type of scan is known as half open because a full TCP three-way connection is not established. This type of scan was originally developed to be stealthy and evade IDS systems although most now detect it. Open ports reply with a SYN/ACK, whereas closed ports respond with a RST/ACK.

TCP FIN scan - This type of scan sends a FIN packet to the target port. Closed ports should send back an RST. This technique is usually effective only on UNIX devices.

TCP NULL scan - a NULL scan sends a packet with no flags set. If the OS has implemented TCP per RFC 793, closed ports will return an RST.

TCP ACK scan - This scan attempts to determine firewall access control list (ACL) rule sets or identify if stateless inspection is being used. If a RST packet returned, it means the port is ether open or closed. If an ICMP destination unreachable, communication administrative prohibited message is returned, the port is considered to be filtered.

NMAP Scan Types (cont)

TCP XMAS - port scan that has toggled on the FIN, URG, and PSH flags. Closed ports should return an RST.

FTP Proxy "bounce attack" scans – bounce an attack off a poorly configured FTP server

Version Scanning – tries to determine the version number of the program listening on the port

Fragmented Scans – can get around some router ACL packet filters that do not examine the port number in fragmented packets.

TCP Sequence Prediction – useful in spoofing attacks

TCP SYN Scan

Client		SYN →	Server
Client	←	SYN/ACK	Server
Client		RST →	Server

```
38194 > netbios-ssn [SYN] Seq=0
netbios-ssn > 38194 [SYN, ACK]
38194 > netbios-ssn [RST] Seq=1
```

- The server is ready but the client never completes the handshake.
- Somewhat stealthy since session handshake is not completed which keeps it out of some log files

Possible responses to a TCP SYN packet

- The server is ready but the client never completes the handshake.
- Somewhat stealthy since session handshake is not completed which keeps it out of some log files

- Open

```
38194 > netbios-ssn [SYN] Seq=0
netbios-ssn > 38194 [SYN, ACK]
38194 > netbios-ssn [RST] Seq=1
```

- Closed

```
44393 > 5001 [SYN] Seq=
5001 > 44393 [RST, ACK]
```

- Filtered (no response)

```
60313 > 203 [SYN]
```

- Filtered (ICMP unreachable)

```
Source port: 7609  Destination port: 7609
Destination unreachable (Port unreachable)
```

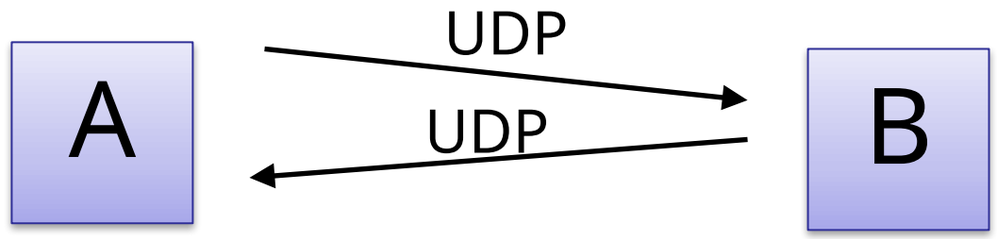
UDP Scan

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port														
4	32	Length																Checksum														

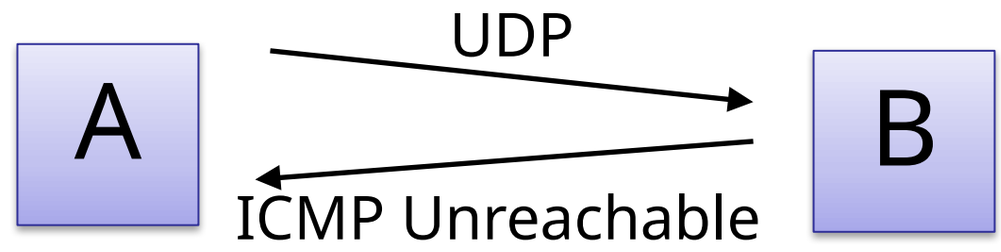
- Much simpler as compared to TCP
- Connectionless
- Less reliable – a response is not assured
- Much slower scanning
  - Some OS limit ICMP unreachable responses
  - Linux limits to 1 per second

Possible responses to a UDP packet

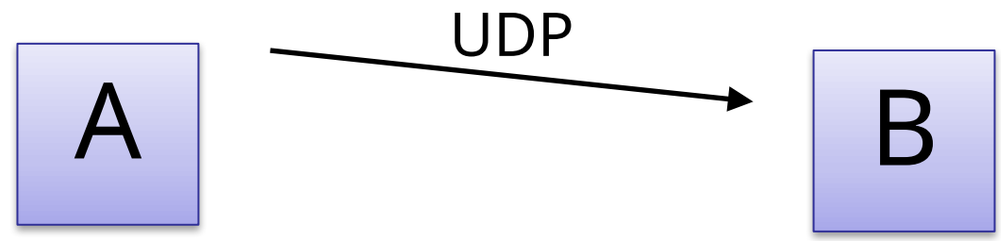
- Open
  - Some ICMP Response



- Closed
  - ICMP Unreachable



- Open|Filtered (no response)
  - Not certain
    - Packet got dropped?
    - Service not responding? (improperly formatted packet)
    - Firewall is blocking



NMAP – ACK Scanning

Some firewalls may allow for outgoing SYN connections and their incoming responses with the ACK bit set.

Stateful firewalls maintain the state of the SYN and ACK packets and will only allow an ACK inbound if there is an outstanding SYN packet.

Can be useful for network mapping

NMAP – FTP Bounce Scan

RFC 959 defines a “feature” in FTP which allows for FTP proxy connections.

Essentially I can connect to a FTP and request the server to send a file to a client.

This should be disabled on properly configured FTP servers.

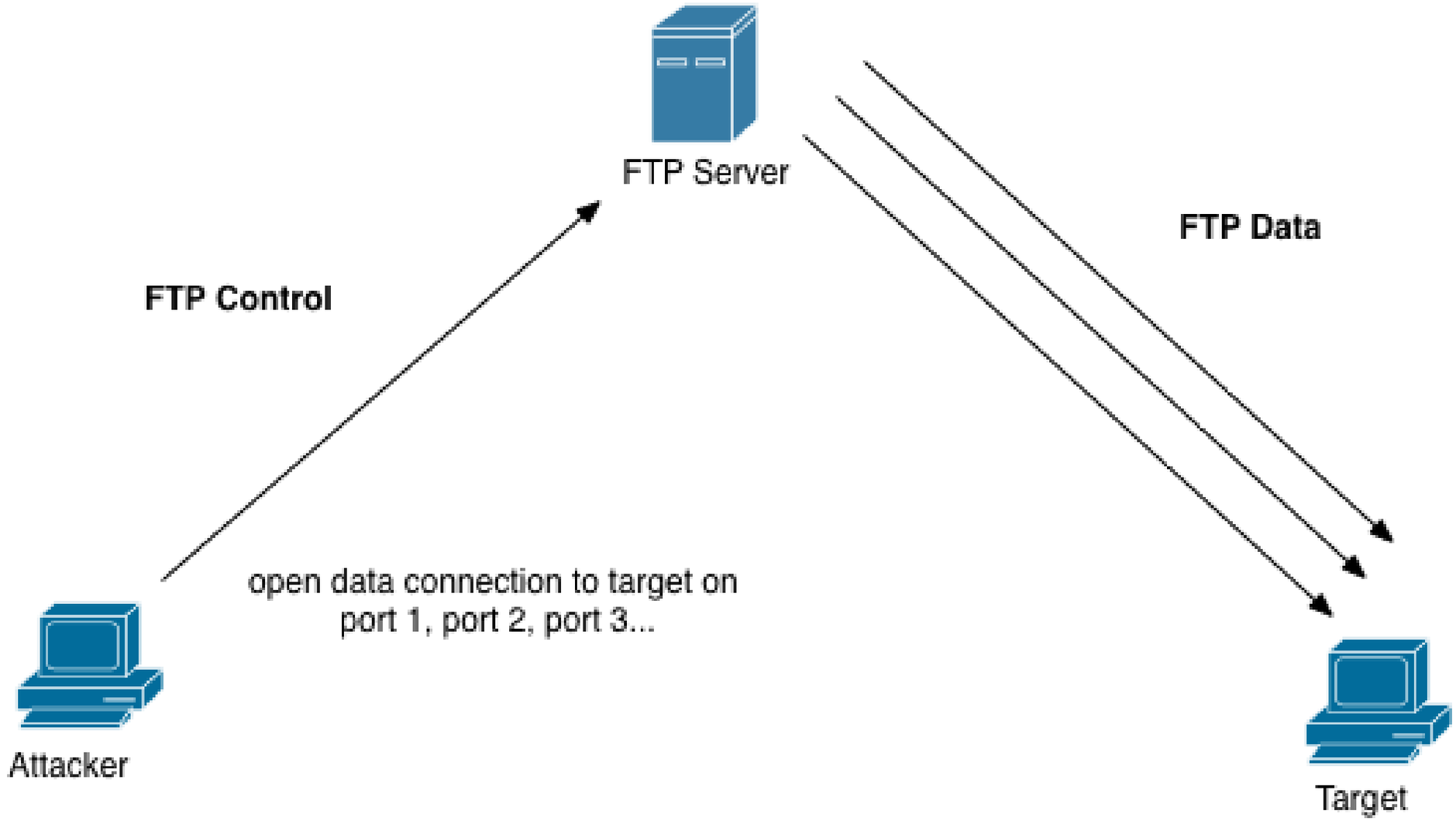
Can be used on misconfigured FTP server to bounce a scan off the server thereby hiding the attackers location.

Use “port” command to try and list directory. If target is listening on the port it will respond with a 150 or 226 response

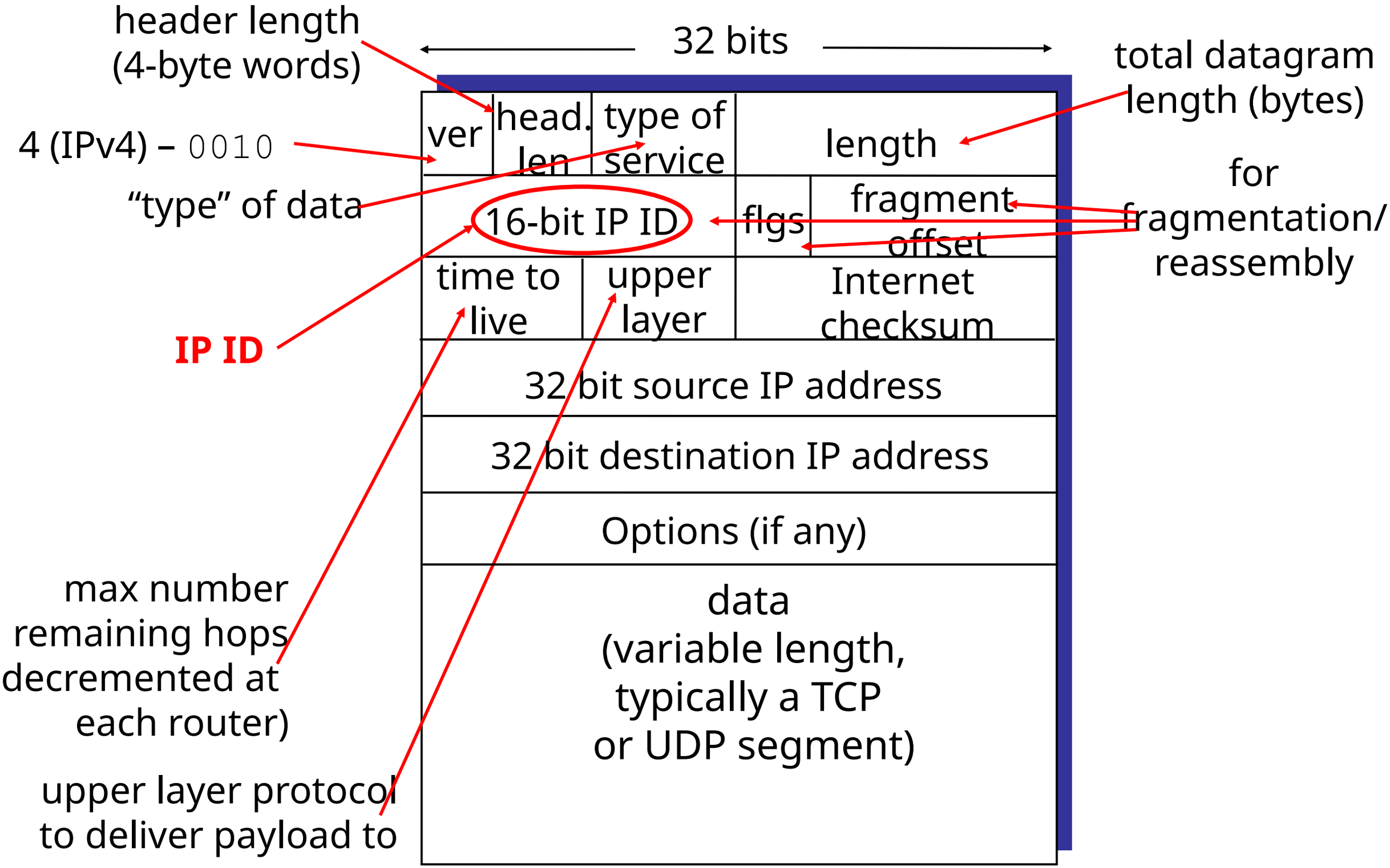
If the port is not listening or closed it will respond with “425 Can't build data connection: Connection refused.”

Useful to get around firewalls if firewall allows connection to FTP server.

FTP Bounce Scan



Interlude: IP datagram format



nmap IDLE Scan (Hide the Scan Source)

Normal port scans send TCP SYN packets to the target and wait for a SYN-ACK

Problem with this is that the attacker is easily identified

If the attacker Spoofs their source IP address then the attacker doesn't't receive the results of the scan.

Use the IP Identification Field of the IP Header.

Normally used to group fragments of IP packets together

Most operating systems increment the IP Ident field by one for each packet sent.

IDLE Scan (cont)

Attacker first picks the machine which will be “framed” for the attack.

Attacker sends a SYN packet to the “framed” machine

Attacker gets back a SYN-ACK which will include the IP header with IP ID value of X which is remembered by the attacker.

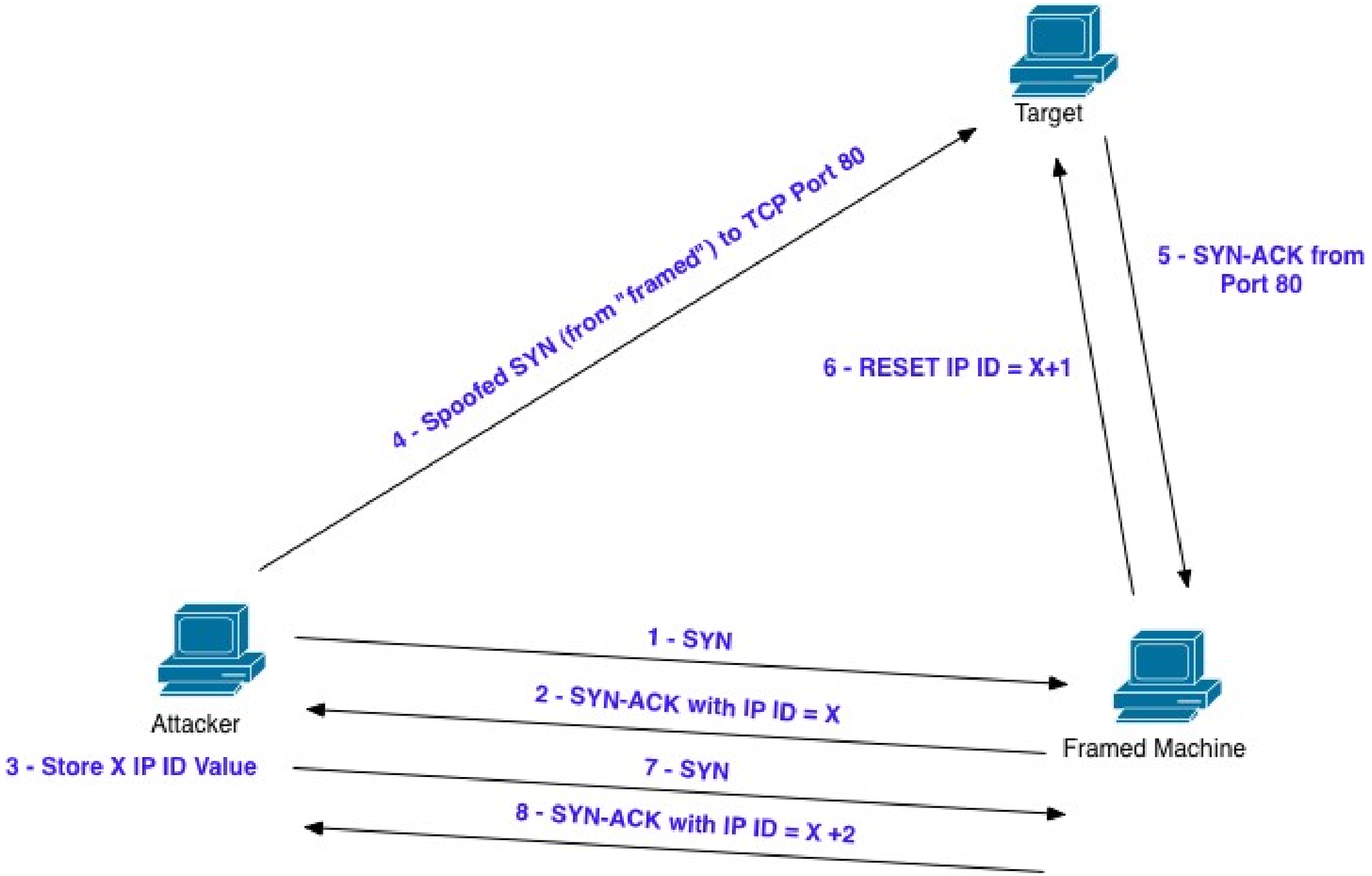
Next step is the attacker selects the port to be scanned and sends a spoofed SYN packet to the target with the “framed” machine’s ip.

If listening the target will send a SYN-ACK back to the framed machine

When the “framed” machine receives a SYN-ACK from the target which was never requested it will send a RESET. The IP ID field on the “framed” machine will be X+1

Attacker now “measures” the IP ID field on the “framed” machine. Sends SYN. If gets IP ID value of X+2 then port is open. If IP ID is X+1 then it is closed

IDLE Scan (cont)



Useful NMAP Command with OS Fingerprinting

```
nmap -sV -O -sC --top-ports 100 -T4 -oA [file] [address]
nmap -sV -O -sC --top-ports 100 -T4 -oA out.txt 10.1.1.0/24
```

`-sV` -Probe open ports to determine service-/version info

`-O` -Enable OS detection

`-sC` -Enable Script scanning

`--top-ports` -Only scan “popular ports”

`-T4` -Sets template for fast scans (0 slow – 5 fast)

`-oA` -Output file

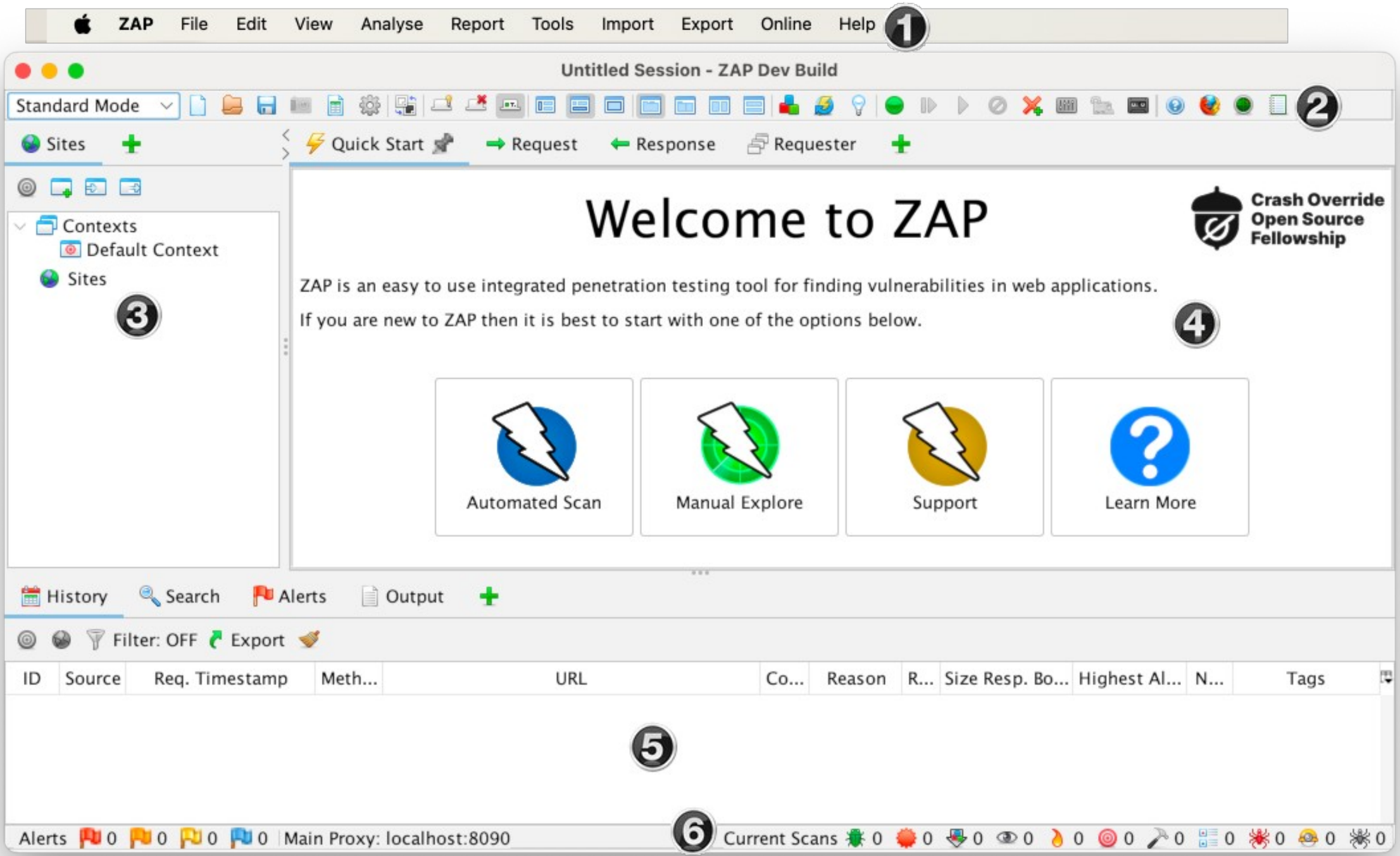
Firewalk

Firewalk is a network scanning tool which attempts to determine which layer3/4 ACLs are present on filtering routers and firewalls.
Sends out TCP and UDP packets with a TTL on greater than the targeted firewall.
If the firewall allows the traffic it will forward to the internal host or next hop where it will expire and return an ICMP_TIME_EXCEEDED message.
If the firewalls drops the traffic no response will be received.

```
firewalk -p [protocol] -d [destination_port] -s [source_port] [internal_IP] [gateway_IP]
```

```
root@fc4>firewalk -n -p tcp -s 80 -d 80 192.168.0.1 192.168.1.1

Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 80, destination port: 80
Hotfoot through 192.168.0.1 using 192.168.1.1 as a metric.
Ramping Phase:
expired [192.168.0.1]
Binding host reached.
Scan bound at 2 hops.
Scanning Phase:

A! open (port not listen) [192.168.1.1]
A! open (port not listen) [192.168.1.1]
A! open (port not listen) [192.168.1.1]
A! open (port not listen) [192.168.1.1]
A! open (port listen) [192.168.1.1]
```

ZAP – Zed Attack Proxy



Summary

At this point we have performed complete reconnaisance on the target network and should have good understand of what is running in the network and how it is designed. Next step is scanning for vulnerabilities which we will cover in the next lecture