Cyber Security

…for Engineers

By J. Mativi

Topics Covered

- The RockYou.com incident analysis
- Passwords and Social Engineering
- Firewalls and Routing
- Networks and VPNs
- Encryption and WiFi Security
- Common Strategies
- Good Practices and Being Safe Online
- Some tools you can use

The RockYou.com Saga

Section 1

RockYou.com

- Allowed users to log in once to gain access to several different social networking or email websites

- Very convenient "one stop shopping" for email and social networking

- It seemed too good to be true…

The Hack

- December 2009
- Over 32,000,000 user account compromised
- Email accounts
- Facebook accounts

RockYou's Mistakes

- Did not properly program their HTML forms
- Very weak password requirements
- Very poor handling of sensitive information and passwords
- Dishonest with their customers

RockYou's Programmers

- The intruder made use of a known MySQL vulnerability that allowed MySQL code to be injected into the database and then executed by entering it into user forms

- This could have been prevented if the RockYou programmers had employed better practices in their coding

The Rockin' Password Policies

- Required 5-15 characters
- Letters and numbers only, no special characters were allowed
- No requirement for mixEd cAsE
- Stored passwords in clear text
- Transmitted password in clear text

Honesty, It’s the Best Policy

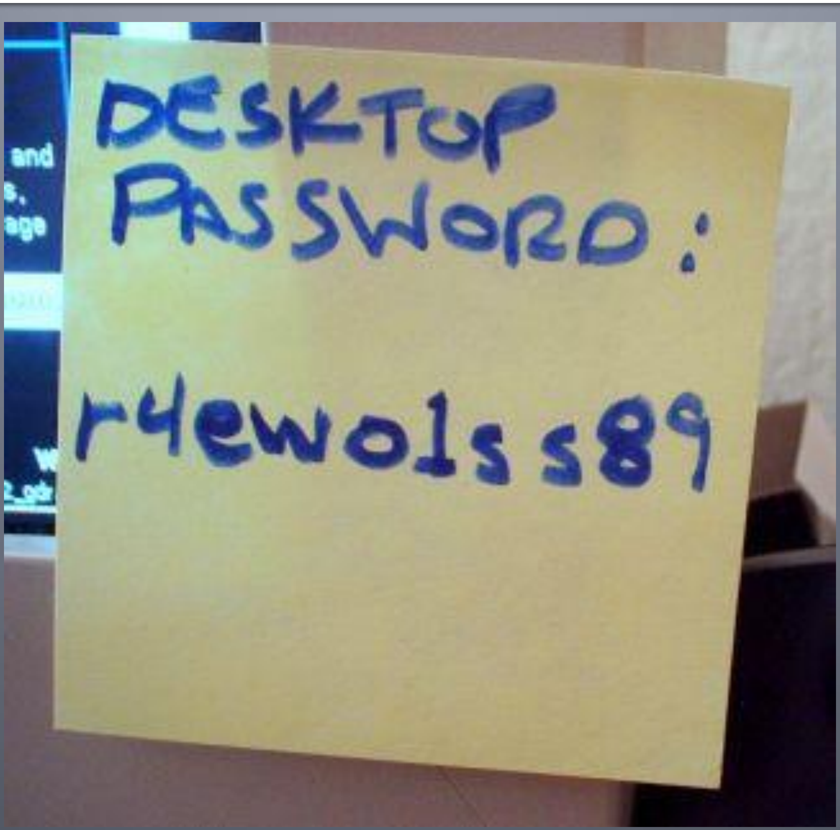
- RockYou told users that their passwords would not be stored
- RockYou downplayed the breach and did not inform users until several days later
- News coverage was kept to a minimum

Mr. Hackerpants Stole My Password. So what?

- Access to:
  - Online Banking accounts
  - Social Networking websites
    - Stalking and Identity theft information
    - Physical Theft
  - Primary E-mail accounts
    - Passwords
    - Fraudulent E-mails
    - Identity Theft

Passwords & Social Engineering

Section 2



http://www.confidenttechnologies.com/files/Post%20it%20note%20password.jpg

Password Please.

- Weakest area of security as they rely entirely on people
- A good password contains:
  - More than 10 characters
  - UPPER and lower case letters
  - Special Characters
  - Long, uncommon, non-sense sentences with numbers
  - A lack of common phrases

You Shall Not Pass!

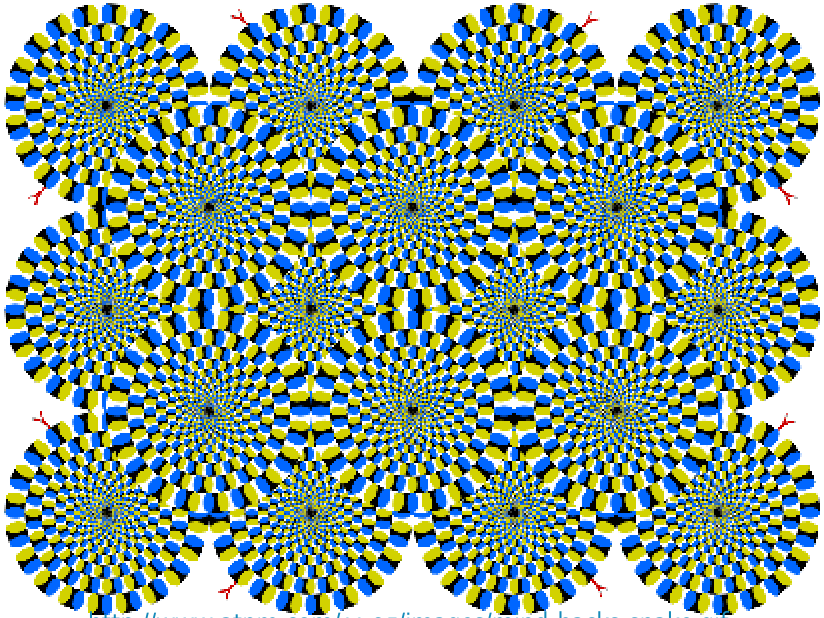
- Examples of good, strong passwords:
  - A%cy763ASfg
  - The300!KittyWarriorsBananaBlueHouse5
  - My1qName2wis3eJohnny4r

Where Shall I Store My Word?

- Passwords should be stored where:
  - No one can read them
  - No one can see them
  - No one can physically touch them
  - No one can photocopy or take a picture of them

Your Mind, or Your Brain

- This is the only safe place to store your passwords.
- Passwords? Plural? Yes. You should have a different password for everything.



http://www.atpm.com/11.05/images/mind-hacks-snake.gif

Some People Need to Know Your Password, Right?

- Wrong. No one other than yourself will ever need to know your password. This specifically includes:
  - Co-workers, your boss, your secretary, and so on
  - Your Internet Service Provider
  - Customer Service Departments (Amazon.com, BestBuy.com, etc)
  - Online Banking
  - The "IT Department"

EPRI's VoIP Phones: An Example

- A convenient feature is the ability to "log in" to your extension from any phone in EPRI
- The default password to do this is 1291
- Users almost never change their passwords
- Logging into someone else's extension allows you to place and receive calls as that person

Clip from "Hackers"

- http://www.youtube.com/watch?v=_G3NT91AWUE

Electrical, Mechanical, Social

- You’re sitting at your desk one day when you receive a phone call…
- John Hackerman is a Social Engineer, and you just gave him access to the company server
- Anyone can be a social engineer. They are capable of getting information from office tours, subtle conversational hints, or your response to certain questions.
- They are professional brain hackers.

Firewalls, Routing, and NAT

Section 3

http://3.bp.blogspot.com/-FzZ5f4TC31Q/T2HwCzBKBCI/AAAAAAAAAFY/eClW6eBDyNQ/s1600/firewall.jpg

Firewalls

- In fancy-talk: A piece or pieces of hardware or software that are designed to prevent unauthorized and unknown access to a digital system
- Put simply: Filters web traffic based on predetermined rules
- Also: A wall made of fire to keep vampires out of your castle

Filtering Options

- Any combination of:
  - Source IP/Domain
  - Destination IP/Domain
  - Port number
  - Packet size
  - Packet Contents

Examples

- Software:
  - Windows Firewall
  - AVG Firewall
  - Zone Alarm Security
- Hardware:
  - SonicWall
  - PIX
  - Routers
- Other:
  - PacketFence

Ports: Not Just from the Douro River Valley

- Ports are similar to exits along a highway. Each exit has a number and brings to you a different place.
- All traffic on the highway has the option of taking an exit.
- Exits are occasionally closed.

Common Port Numbers

Port(s)	Use
80, 8080	HTTP
443	HTTPS
23	Telnet
20, 21	FTP
25	SMTP
445	Active Directory, MSWin Filesharing
666	Doom
992	Secure Telnet (TLS/SSL)

Protocols

- Two major protocol suites in use on the internet: TCP/IP and UDP
- TCP/IP (Transmission Control Protocol / Internet Protocol)
  - Used for most web traffic
  - Reliable but not the quickest way to get things done
- UDP (User Datagram Protocol)
  - Compliments TCP/IP
  - Faster but less reliable

Routers

- Route and direct traffic from the small, personal level all the way to large-scale, global levels.

- Traffic is directed based chiefly upon Network Address/Subnet Mask and Source/Destinaton information.
- Routes both private and public traffic.

The Day the Routers Died

- http://www.youtube.com/watch?v=_y36fG2Obao

- Without routers, internet traffic would get nowhere. Global communication would fall back to HAMs and other forms of radio and switchboard communication

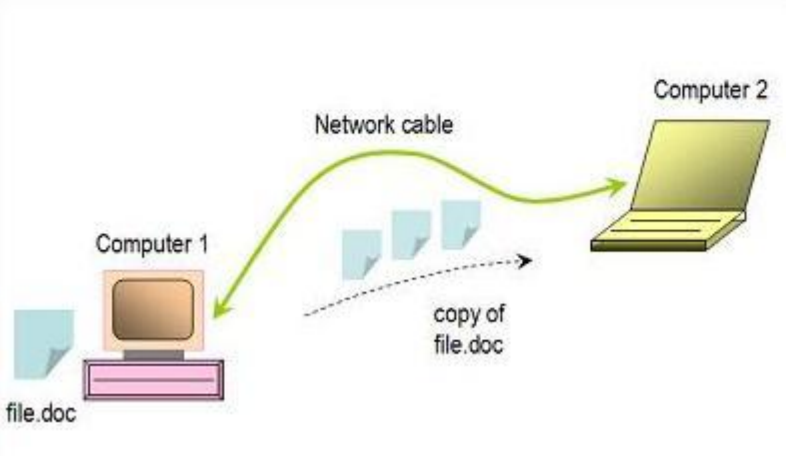
Look Over There! What's NAT?!

- Network Address Translation is a built-in layer of security for consumer level routers.

- NAT takes your public IP address (similar to your house, which everyone driving by can see) and converts it into a private address (similar to rooms within your house, only seen by trusted people)

Networks

- At it simplest, a network is two computers that are connected to each other and able to communicate.
- The internet is not just that strange netting inside swim shorts: it is a world-wide network of computers.



http://compnetworking.about.com/library/graphics/basics_simplenetwork.jpg

IP Addresses

- A binary way to assign a computer's Network Interface Card a numerical "name", allowing other similarly named computers to communicate with it.
- Two parts to each IP address
  - Network: the network to which the address belongs
  - Host: the specific machine to which the address belongs
- The Network and Host portions are differentiated by the subnet mask

Here's an Example

- The IP Address 192.168.1.58/24
- The /24 indicates that the first 24 bits of this address are the network portion and the remaining 8 bits are the host portion. This is the subnet mask. It could also be written as 255.255.255.0
- 11000000.10101000.00000001.00111010
- 1 9 2 . 1 6 8 . 1 . 5 8

In the Beginning…

- Networks were classy and had implied subnet masks
  - Class A
    - Starts with 0-127 (0), /8
  - Class B
    - Starts with 128-191 (10), /16
  - Class C
    - Starts with 192-223 (11), /24
  - Class D, E – Multicast, Experimental, Reserved

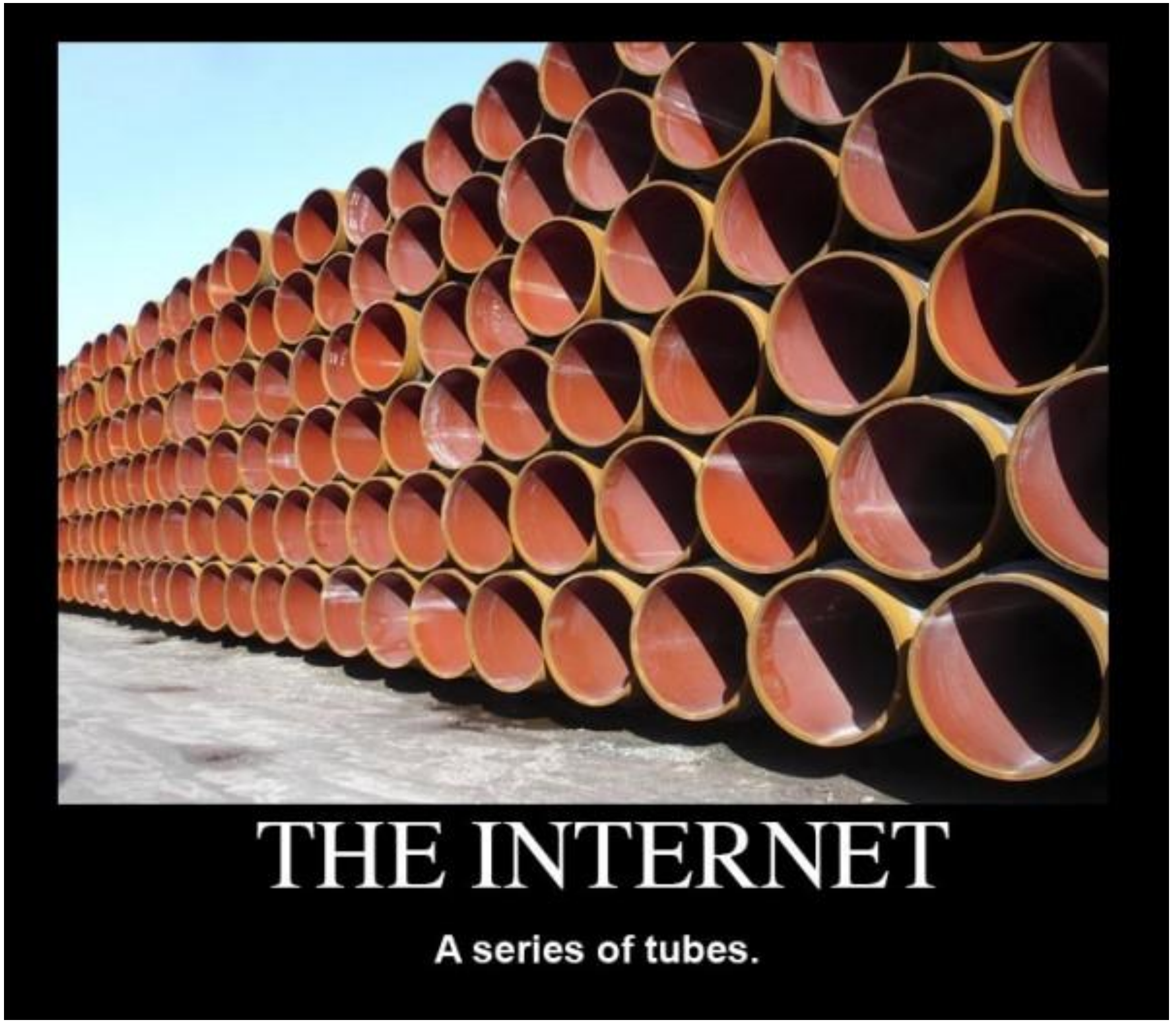
CIDR

- Classless Inter-Domain Routing changed the way networks talk to each other, and provided an alternate spelling of the word "Cider".
- IP Addresses no longer had to use their implied subnet masks.
- Introduced to option of Variable Length Subnet Masking (VLSM)

The Internet!

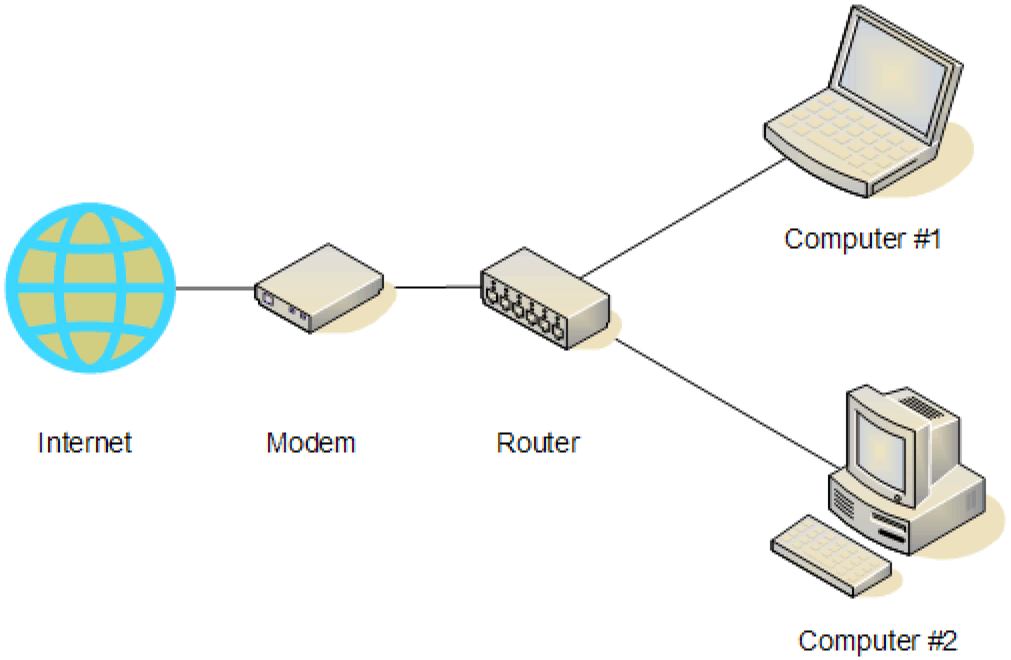
- The star was officially born in 1982 with the standardization of the TCP/IP stack.
- A public, world-wide network of networks, clients, servers, routers, switches, firewalls, and conspiracy theorists.
- Online content is delivered from a computer, or server, somewhere in the world to you, the client, when you browse a web site.

Alaskan Senator Ted Stevens says…



http://ctovision.com/wp-content/uploads/2011/12/the-internet-a-series-of-tubes-e1302137805665.jpg

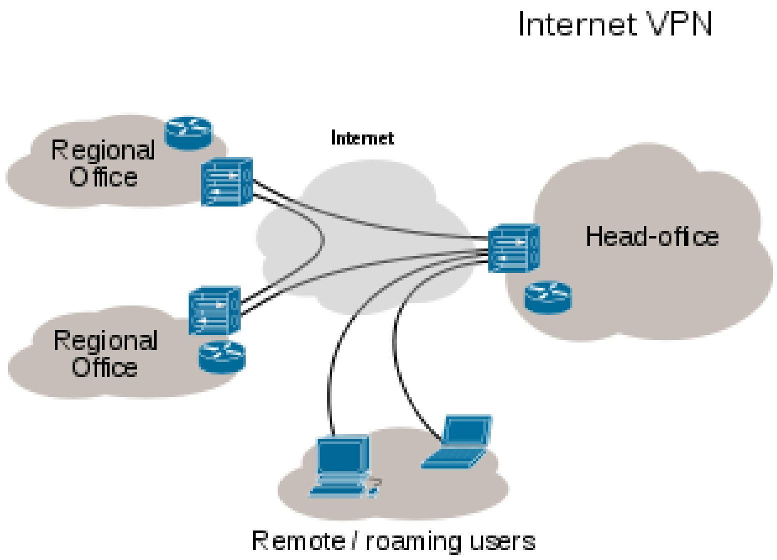
Put Simply…



http://www.ustudy.in/sites/default/files/images/internet.gif

VPN – Virtual Private Networks

- A private, local network created over the internet allowing remote user computers to behave as though they were local.



http://upload.wikimedia.org/wikipedia/commons/thumb/0/00/Virtual_Private_Network_overview.svg/330px-Virtual_Private_Network_overview.svg.png

VPNs Add a Layer of Security

- Connections to a VPN are encrypted
- Data sent over a VPN is encrypted
- Local resources no longer need to be configured for remote access
- HTTPS, SSL, and other common security measures can still be implemented

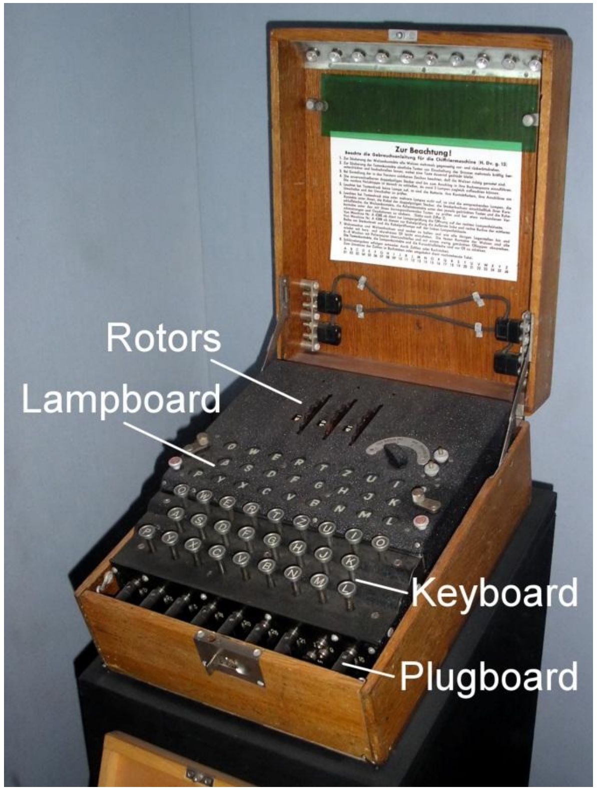
Encryption & WiFi Security

Section 5

http://sophosnews.files.wordpress.com/2011/02/data-encryption.jpg?w=640

Data and Connection Encryption

- Encryption is the process of altering information using a known method to prevent dissemination of that information without knowing the method by which it was altered.
- Put simply: Figure out a way to tweak your information so other people can't "just read it".



http://upload.wikimedia.org/wikipedia/commons/3/3e/EnigmaMachineLabeled.jpg

How it’s Done, Part 1: Handshakes

- The Handshake: A friendly “howdy do” between two different parties or computer systems.
  - The client sends a request.
  - The Access Point (in the case of WiFi) replies with a clear-text challenge.
  - The client encrypts the challenge using the WEP key it was given and sends it back to the AP.
  - The AP decrypts and compares the response to its original challenge

How it's Done, Part 2: [Stream] Cyphers

- A stream of plaintext information is hashed up against a pseudorandom stream of "key" characters, to be deciphered at the receiving end. Example: WEP.
- Pseudorandom: Appears random but is generated via a know process and variable set

http://1.bp.blogspot.com/_SwSLDhWV6vU/TTAQDWxF9vI/AAAAAAAAADw/vMH1PpR3B4g/s1600/cypher.jpg

WiFi Encryption - WEP

- Wired Equivalency Protocol
- Early security algorithm for IEEE Standard 802.11
- 40bit, or “WEP 40”
  - Key composed of 10 hex characters
- 104bit
  - Key composed of 26 hex characters
- Easily broken by
  - Analyzing captured packets
  - Knowing, guessing, or cracking the WEP key

WiFi Encryption – WPA 1 & 2

- WiFi Protected Access, v1
  - IEEE Standard 802.11i
  - Utilized temporal key generation via the Temporal Key Integrity Protocol (TKIP)
- WPA 2
  - IEEE Standard 802.11i-2004
  - Added Advanced Encryption Standards (AES) in addition to TKIP

WiFi Protected Setup: Making Life Easier – for Everyone

- Initially designed and implemented as a means for users with a low level of knowledge to implement their own WiFi security.
- The WPS PIN method of security is vulnerable to brute force attacks.
- You're only safe if WPS is disabled or not supported by your router.
- Just pay a geek to do it, it's less of a headache.

Have a Backbone!

- At its core, the “Backbone” of the internet is wired, not wireless.
- Similar security protocols are enacted, but with less necessity.
- More secure than WiFi since access requires a physical interface and can be easily patrolled.
- Less prone to interference and capable of much higher speeds.

Attack! Defend!

Section 6

http://s3.amazonaws.com/readers/2011/09/10/hackedskullimage_1.jpg

Common Attack Strategies

- MS-DOS, DoS, DDoS
- Usurping the Server
- Man-in-the-Middle
- Sniff & Snap
- Brute Force
- Nuking (Once entry is gained)

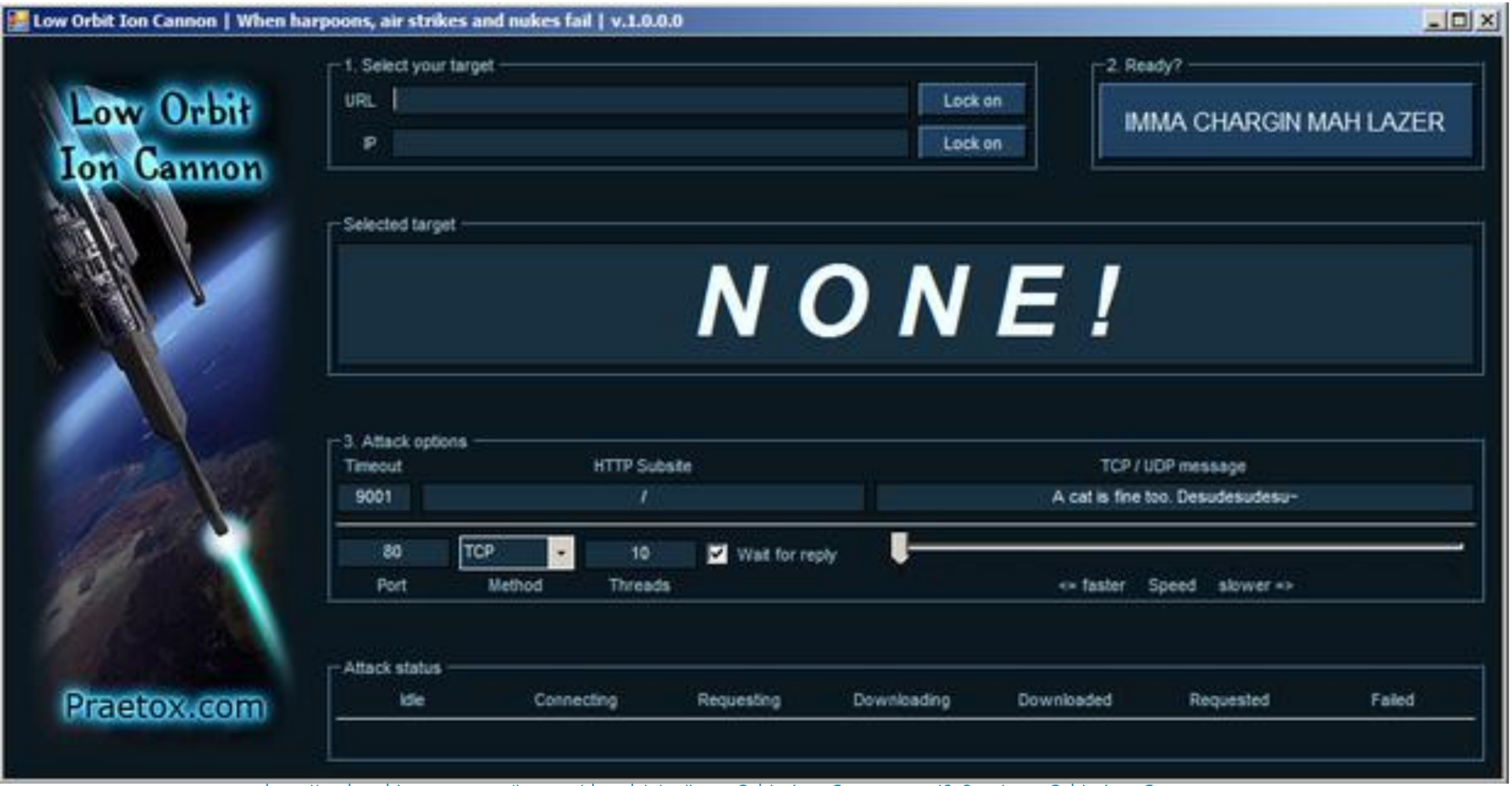
DoS & DDos

- [Distributed] Denial of Service attack
- Aims to cripple a target, usually a server, by overwhelming it with requests, effectively stopping it from communicating with other clients.
- This requires clients, and lots of them, to remain active and attempting to connect to the target for the duration of the attack.

A Recent Example

- In January of 2012, in response to the Federal shutdown of megaupload.com and the growing concerns of SOPA, the “Hacktivist” group called Anonymous took down several government servers. These included the Department of Justice website and the FBI website. This was done using an DDoS attack program called the Low Orbit Ion Cann (LOIC).

The Weapon of Choice



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

1. Select your target

URL

IP

Selected target

NONE!

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

Method: TCP

Threads: 10

☑ Wait for reply

http://cache.ohinternet.com/images/thumb/1/10/Low_Orbit_Ion_Cannon.png/618px-Low_Orbit_Ion_Cannon.png

The Dee Daus Defense

- Servers that do not respond to ping requests.
- Limiting the number of connects to a server, and having that server drop timed out connections.
- Filtering traffic
  - Usually based on content or timeout duration
- A very diligent network administrator to kill suspected DoS connections and report them.

Usurping the Server

- In this scenario the attacker will attempt to gain control of a server.
- Usually done by obtaining a password, port scanning, and using the password.
- Server control via remote desktop (or equivalent) or SSH.
- The attacker can do just about anything they want once inside a trusted server.

Quelling the Revolution

- The most common defense for this is called a Honeypot Trap.
- Using a purposefully vulnerable server and loading it with important-looking dummy data to trap any attackers.
- Once the attacker is in the Honeypot Trap, all of their information is recorded and reported. Hopefully they are trapped long enough to figure out who they are.

Man-in-the-Middle & Sniffing

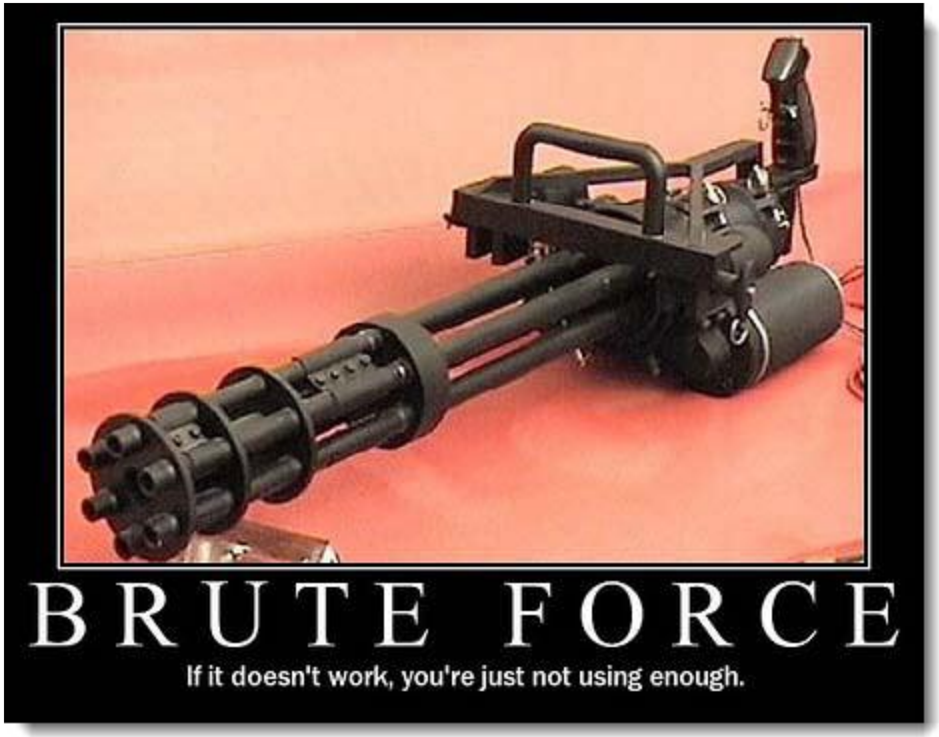
- The Middle Man Attack: a foreign user attempts to insert himself into the communication path of a network and capture packets, sending false information to the clients.
- Packet Sniffing: Capturing transmitted packets and analyzing them to break at WEP key or to spoof information to users or authentication points.

Cutting out the Middle Man

- The best defense against Sniffing and Middle Man attacks is to limit your network access.
- Allow only specific machines to access your network.
- Require encrypted connections (VPN is an easy way to do this).
- Transmit encrypted data.
- Enforce TTL/Latency timers.

Brawn over Brains

- Brute Force attacks are a process of elimination, trying every possible combination of a password or key until the right one is found.



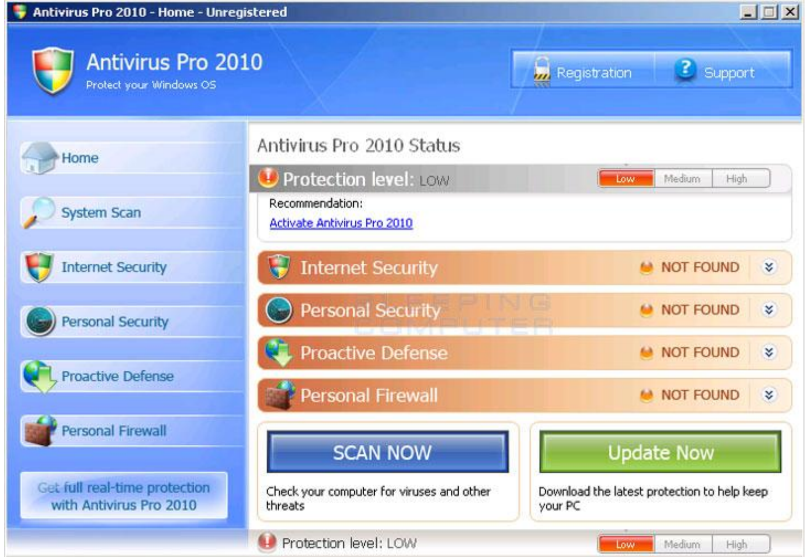
http://4.bp.blogspot.com/_F2z9HWqGZU/TUA5Ib9NN8I/AAAAAAAACe8/n4ZrY1sv97Y/s1600/Brute-Force-Attack.jpg

Brains over Brawn

- Strong passwords or encryption keys make Brute Force attacks easier to stop.
- Administrators that see multiple failed attempts *should* drop the Ban Hammer on the source of these attempts.
- Limiting network access or machine access is also helpful.

Malicious Software

- Rootkits
  - Malware that obtains Administrator privileges and uses them to hide itself and prevent removal.
- Browser Redirects
- HOSTS File Edits
- Fake AntiVirus Software
  - Antivirus Professional 2010
  - Often aimed at stealing credit card info



Antivirus Pro 2010 - Home - Unregistered

Antivirus Pro 2010
Protect your Windows OS

Antivirus Pro 2010 Status

Protection level: LOW

Recommendation:
Activate Antivirus Pro 2010

Internet Security	NOT FOUND
Personal Security	NOT FOUND
Proactive Defense	NOT FOUND
Personal Firewall	NOT FOUND

Check your computer for viruses and other threats

Download the latest protection to help keep your PC

Get full real-time protection with Antivirus Pro 2010

Protection level: LOW

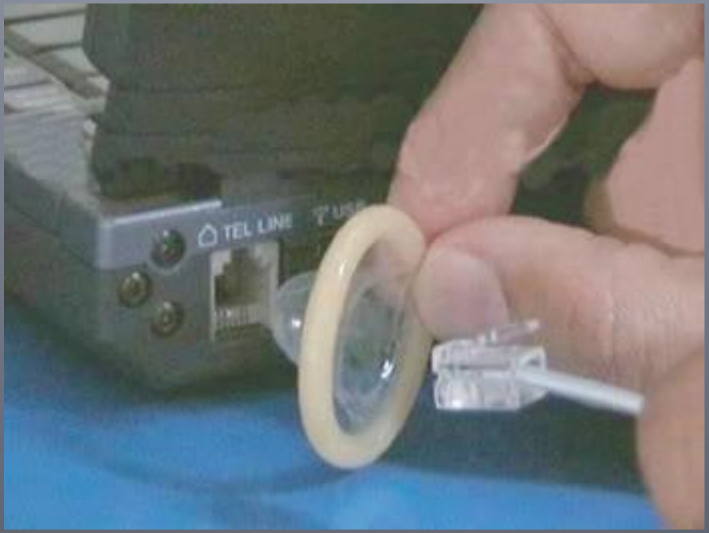
http://www.bleepstatic.com/swr-guides/a/antivirus-pro-2010/antivirus-pro-2010.jpg

The Digital Anti-viral Treatment

- There are 3 good ways to stop infections of viruses, malware, etc:
  - Human Vigilance, this is the most important. Don’t fall for their tricks.
  - A good AntiVirus software
    - AVG
    - SpyBot Search & Destroy
    - Malwarebyte’s Antimalware
  - Know a good geek and offer them money

How to be Safe on the Internet

Section 7



Security Lockdown

- When you’re not at your computer, lock it. (Windows + L)
- If you use a Smartphone to access email or do online banking, use a password, PIN, pattern, or facial recognition lock on the phone.
- Use strong passwords, only store them in your brain, and never give them out to anyone.

E-Mail Awareness

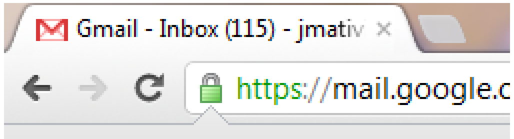
- Do not click links in emails. Iff you must, check the link's actual URL first.
- Just because it wasn't flagged as SPAM does not mean it is safe.
- Just because it is from, or appears to be from someone you know, does not mean it is safe.
- Never send your password in email. Ever. For any reason.
- You are not the 1 millionth visitor, you did not inherit a fortune from a some Pakistani prince, you did not qualify for a free trial of an experimental penis enlargement pill, and your information does not need to be updated.

Attachments & Extensions

- .exe, .bat, and .com file extensions are executables. Open them at your own risk! Watch out for links that contain files with these extensions.
- If a file ends with .exe, .bat, or .com it is not an image, or document, or powerpoint. Don't believe it just because your friend John emailed you and said it's a picture of the two of you.

Web Browsing & Online Purchasing

- Be cautious when sending sensitive information over the internet.
- This includes credit card information, social security numbers, your home address, passwords, and where you leave the hide-a-key.
- Check first for a secure connection (HTTPS) before you send.



https://mail.google.c

Logging Into Websites

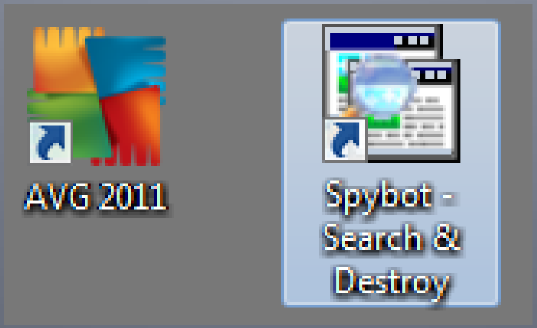
- Once you're done, log out! There is no need to leave your facebook page or walmart.com shopping cart open in a browser and still logged in. You are asking for trouble.

Domain Extensions

Trustworthy	Not So Trustworthy
.edu	.info
.gov	.biz
.org	.tk
.net	.xxx
.com (not always)	.pro

Tools to Help You Stay Safe

Section 8



AntiVirus & Anti Spyware

- AVG AntiVirus
  - Free and effective
  - Updates regularly
  - Has the option for a more complete solution, with payment
- SpyBot Search & Destroy
  - Free, regularly updated
  - Removes browser hijackers, malware, spyware, etc
- Windows Firewall
  - Basic online protection, included with Windows XP +

Questions

Does anyone have any?