What You Expect
Common Hacker Techniques

- Direct Break-In
- Man-In-The-Middle
  - DNS Spoofing
  - Rogue Access Points
  - Connection Hijacking
Direct Break-In
Direct Break-In Defense

○ Windows
  ● Built In Firewall in XP
  ● Third Party Software Firewall
    ○ Kerio Personal Firewall
    ○ ZoneAlarm
    ○ Sygate Personal Firewall

○ Linux/UNIX
  ● Turn off unused services
  ● TCP wrappers
  ● IPfilter (Solaris, BSDs)
  ● IPtables (Linux)
XP Firewall (pre SP2)

1. Right click
2. Internet Connection Firewall
3. Settings
4. Services: Iprng, 7123 TCP, 11902 UDP

Select the services running on your network that Internet users can access.
XP SP2 Firewall
Man-In-The-Middle
Man-In-The-Middle Defense

Everything in SSL (check that certificate)

- www.megaproxy.com

Use some sort of Virtual Private Networking (VPN)

- Creates an encrypted tunnel between you and some other server
  - Encryption hides what sites you are accessing
  - Encryption is tamper resistant
- Most often used for remote access
SSL: the Certificate Check Should Alert You to Tampering

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- The security certificate is from a trusted certifying authority.
- The security certificate date is valid.
- The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

[Yes] [No] [View Certificate]
How VPN changes access

YOU

INTERNET

www.yahoo.com

www.cnn.com

DNS server

VPN server
How do I get a VPN?

- Have an employer that supplies a remote access solution
- Roll Your Own – Do It Yourself
  It’s not difficult
An Employer Supplied VPN

- **Pros**
  - They did most of the work and/or paid for the solution
  - You might get support
  - May protect you from questionable websites

- **Cons**
  - May only be available for Windows hosts
  - You’re not really on the internet anymore
  - May restricted you from any number of websites
  - Privacy: employer might record all sites you access
  - Policy: employer might disallow this type of use
Need to use employers proxies
Employer Filtering

Blocked Site

http://www.hotbar.com/

Access to this site has been blocked because it appears to contain material that is either inconsistent with the Principles or could present a risk to Security.

Please refer to the Guidelines for Electronic Communications or call Information Security & Privacy if you require further information.

The WebSense category "Spyware" is filtered.

Blocked Site

http://www.defcon.org/

Access to this site has been blocked because it appears to contain material that is either inconsistent with the Principles or could present a risk to Security.

Please refer to the Guidelines for Electronic Communications or call Information Security & Privacy if you require further information.

The WebSense category "Hacking" is filtered.

Blocked Site

http://www.broadbandreports.com/forum/vpn

Access to this site has been blocked because it appears to contain material that is either inconsistent with the Principles or could present a risk to Security.

Please refer to the Guidelines for Electronic Communications or call Information Security & Privacy if you require further information.

The WebSense category "Message Boards and Chats" is filtered.

Blocked Site

http://mail.google.com/

Access to this site has been blocked because it appears to contain material that is either inconsistent with the Principles or could present a risk to Security.

Please refer to the Guidelines for Electronic Communications or call Information Security & Privacy if you require further information.

The WebSense category "Web-based Email" is filtered.
Roll Your Own – Do It Yourself

Easier Than You Think
- Microsoft VPN
- Use SSH tunnels
  - Works under Windows
  - Works under UNIX/Linux
  - Works under Macs
- Requires another computer you trust somewhere else on the Internet
  - At your home
  - Collocated at a hosting facility or ISP
  - Purchase a shell account
Microsoft VPN

- Windows has a built-in VPN, Microsoft’s PPTP
- It seems to have some security flaws
- UNIX/Linux client: PPTP Client
- UNIX/Linux server: Poptop
- Cisco routers and firewalls can talk it too
- Uses a modified GRE/IP (not TCP/IP)
- If you only want to secure web browsing there’s an easier way that’s more secure
VPN with SSH

- SSH is Secure SHell
  - Available on just about every platform
  - Commonly considered “encrypted telnet”
  - But has much more
    - Has port tunneling capability built in
    - Has a SOCKS server built in
  - There’s two versions: 1 and 2
    - Use version 2
      - Use a newer server, there were some flaws in older implementations
  - Easy to use
  - Only uses a single TCP/IP port (default is 22)
  - No problems with Network Address Translation (NAT)
SSH Software

- **Client**
  - SSH
    - Comes standard on UNIX/Linux/Mac OS X
    - Free Windows clients: PuTTY
      - Easy download, no install (no admin rights needed)

- **Server**
  - SSHD on a remote host
    - Comes standard on UNIX/Linux
    - Free Windows server: opensshd
      - Easy download and install
Remote is UNIX/Linux

- SSHD is all ready there, just use it
- Use an any account you can log into (root account not recommended)
- Buy a shell account that allows you to ssh into (e.g. panix offers one at $10/month or $100/year)
Remote is Windows

- Install and start it
  - net start openssd
- Or if you currently use cygwin (ignore if you don’t know what this is)
  - Download these packages -
    - `openssh`
    - `cygrunsrv`
    - `perl` (not need for ssh, but we’ll use it later)
  - Configure it with ssh-host-config in a cygwin shell
    - Answer privilege separation “no”
    - Answer CYGWIN= “ntsec tty”
  - Start service with cygrunsrv –S sshd
- Windows user account MUST have a password
Remote is Windows XP (pre SP2)
Accept connections on port 22 (part 1)
Remote is Windows XP (pre SP2)
Accept connections on port 22 (part 2)
Remote is Windows XP SP2
Accept connections on port 22
Remote is Windows XP SP2
Accept connections on port 22
Open Inbound Port 22 on External Firewalls

Home users: remember to open up and map port 22 on your router/firewall to your internal server.
Client: Start SSH with SOCKS

- UNIX/Linux:
  
  $$ \texttt{ssh \textendash D9119 user@remote-host.com} $$

- Windows: PuTTY
Have the SSH key before hand

- First time use will prime key on client side
- UNIX/Linux/Cygwin –
  
  $ ssh cuzuco.com
  
  The authenticity of host 'cuzuco.com (196.12.190.248)' can't be established.
  Are you sure you want to continue connecting (yes/no)?

- Windows (PuTTY) –

![PuTTY Security Alert]

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's dss key fingerprint is:

```
```

If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
Server key is different (probable attack)

- UNIX/Linux/Cygwin -
  
  ```
  $ ssh cuzuco.com
  WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!
  IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
  Someone could be eavesdropping on you right now (man-in-the-middle attack)!
  It is also possible that the DSA host key has just been changed.
  The fingerprint for the DSA key sent by the remote host is 2b:84:cb:4a:d0:ea:05:f3:50:3a:96:f3:47:61:01:3d.
  Please contact your system administrator.
  Add correct host key in /net/u/16/b/bsw/.ssh/known_hosts to get rid of this message.
  Offending key in /net/u/16/b/bsw/.ssh/known_hosts:90
  DSA host key for cuzuco.com has changed and you have requested strict checking.
  Host key verification failed.
  ```
Server key is different (probable attack)

- Windows (PuTTY) –
Firefox to use SOCKS
IE to use SOCKS
My home IP address changes all the time

- Use a free dynamic DNS service such as
  - dyndns.org
  - zoneedit.com
- Use an agent on your machine to automatically update the IP to a static name or it maybe built into your router.
Client does a DNS lookup and then sends that IP to the SOCKS server. DNS spoof attack may still succeed.
Use A Proxy Server as well
PROXY Software

- **Client**
  - Nothing need: It’s built into the browser

- **Server**
  - UNIX/Linux
    - Simple perl program
    - or-
    - Squid
  - Windows
    - Simple perl program (requires Cygwin or ActiveState perl installed)
    - or-
    - FreeProxy
  - There’s no shortage of proxy server software written in C, perl, or java
Get the perl proxy

Can be found at

http://www.cis.upenn.edu/sdt/proxy.pl
-or-
http://www.cs.princeton.edu/~dabo/proxy/proxy.pl

Make a small edit

change

require "sys/socket.ph";

to

use Socket;
Perl for windows

- If you are running Cygwin you probably all ready have perl
- Otherwise you can download a free copy from ActiveState
  [http://www.activestate.com/Products/Download/Download.plex?id=ActivePerl](http://www.activestate.com/Products/Download/Download.plex?id=ActivePerl)
- Alternatively if you have to download something, you can just get FreeProxy instead of perl binaries and the perl proxy program
Client: Start SSH with tunnel

- UNIX/Linux/Cygwin:
  $ ssh -L8080:127.0.0.1:5364 user@remote-host.com

- Windows: PuTTY

  - If using FreeProxy change the number 5364 to 8080
Running The Proxy

- SSH into the remote machine
- Windows run -
  - If using FreeProxy, must start it before
  - If using perl
    \perl\bin\perl proxy.pl
- UNIX/Linux/Cygwin run -
  $ perl proxy.pl
Firefox to use perl proxy
IE to use perl proxy
Perl Proxy does not support SSL Pass-through.

Standard access (non-SSL) goes through proxy.

SSL access goes direct.
No SSL support is not that bad

- Since SSL is one of the ways you can secure yourself, only DNS spoofing can happen.
- Just watch for sites that have certificate problems (as noted previously).
- Or use a proxy server that supports SSL pass through (FreeProxy, squid).
Performance Considerations

○ CPU
  - Encryption uses CPU cycles on both the client and server
  - Usually only an issue if you have many clients on a single slow server

○ Bandwidth
  - The server must relay all traffic (doubles the data)
  - The server’s upload speed becomes the maximum download speed (think home DSL line with slow upload)
Other Considerations

- VPN tunnels require continuous communication
  - If you roam from one AP to another, your session will disconnect and you have to reconnect it
  - If you lose association to the AP for any reason (weak signal, noisy radio environment, AP reboots) your session will disconnect and you have to reconnect it

- If you need more than just web browsing you may need a full VPN
  - PPTP
  - IPSec
Full VPN Combinations

- **YOU**
  - Windows native PPTP client

- **YOU**
  - UNIX/Linux PPTP Client (open source)

- **YOU**
  - Windows native PPTP server

- **YOU**
  - UNIX/Linux FreeS/Wan or OpenSWAN

- **INTERNET**
  - VPN server

- **INTERNET**
  - VPN server

- **INTERNET**
  - UNIX/Linux Poptop server

- **INTERNET**
  - UNIX/Linux FreeS/Wan or OpenSWAN
Other Good Ideas

- Use Anti-Virus software
  - AntiVir
  - AVG Anti-Virus
- Use Anti-Spyware
  - Spybot Search & Destroy
  - Ad-Aware
- Use Anti-Browser Spoofing and Hijacking
  - Spoofstick
  - Ad-Aware
- Don’t Use IE
  - Firefox
  - Maxthon (was MyIE2)
- Don’t Use Outlook
  - Thunderbird
Not limited to just Wi-Fi

- These techniques can be used on any network not trusted, wired or not.
- Can also be used to tunnel out from restricted networks.
- You don’t have to use port 22 for sshd, you can use any unused port. You can put it on 443 if you are not running an SSL web server. This port is always allowed out through proxies. You can run it on a random high port to “hide” it.
Stuck on the Corporate LAN/VPN? SSH tunnel out
PuTTY can Tunnel Through Proxy

1. Select Proxy
2. Choose HTTP
3. Enter com as Proxy hostname
4. Enter 8080 as Port
We’re Done

- All software noted in this document is available at no cost
- The links for all of the software, references and services can be found at [http://wifidefense.cuzuco.com/](http://wifidefense.cuzuco.com/)
- The home router/firewall/access point screens are from a Linksys WRT54GS