

Anti-Whaling

Hardening up your “net” presence



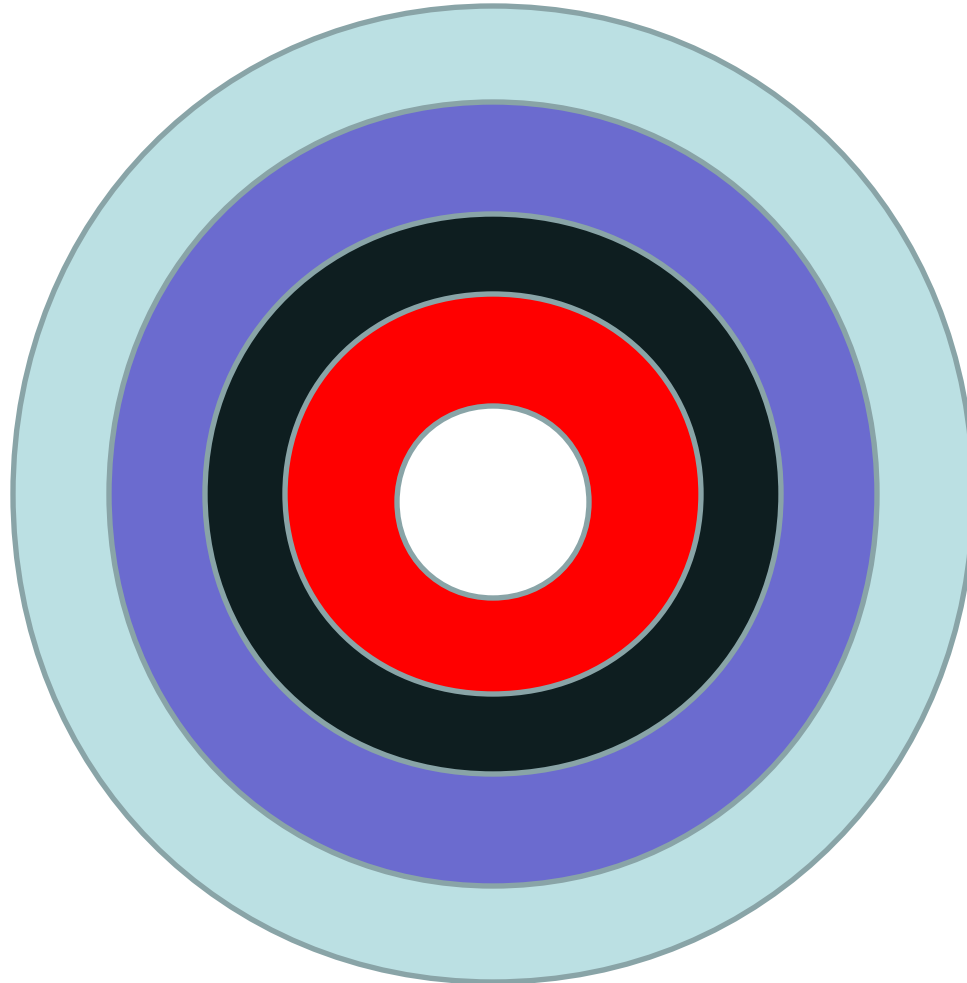
A quick survey

- How many of you use the Internet in your business?
- How many of you have hi speed internet ADSL at home?
- How many of you use wireless?
- How many of you own a phone?
- How many of you use a GPS?

Whaling...

- Targeted attacking of a high worth individual by cyber criminals
- Bad news people you are most probably in the target market....
 - You control critical infrastructure
 - You have information that is valuable, plans, bids, contracts, private communications
 - Your incomes are eventually in the medium to high end

Defence in Depth



Edith Cowan University

Policy is at least a plan

- Policy should inform your decisions its your strategic intent and risk
- Procedures should relate to your policy
- Processes and people are just as much part of your security or insecurity as the hardware and software

Practicing Safe Hex

- The Internet is an increasingly hostile place
 - Malcode – viruses, worms
 - Attack tools and knowledge sharing
 - Social engineering
 - Interception
 - Identity Theft
 - Pipes are getting bigger
- You need to make yourself a hard target

Malcode Protection

- Some protection is better than none
- Where possible use 2 different virus engines in a business
- Always update every day as a minimum
- Unless you are expecting an attachment do not open it...
- Do not follow links in an email **EVER**
- Use and install a spyware detector

Firewalls

- Firewalls have a place **TURN THEM ON!**
- But suffer from Bastille Mentality
- Provide a good second layer of defence
- However many of the new exploits bypass these
 - Keylogging
 - Mouse Logging
 - Screen Relay

Attack tools

- Are increasingly available and easy to use, luckily in this state possession of same is now a problem for you
- Are very effective at penetrating insecure systems or systems badly out of patch...
- Metasploit, Nessus, Nmap



Knowledge sharing

- Hackers hunt in packs
- Websites are just one avenue for dissemination of information
 - Online chats – irc, skype etc
 - File dumps
 - Virtual servers
- The ultimate goal of a hacker is a “zero day”



Social Engineering

- Social sites are great avenue for this..
- Email is then constructed that can contain payloads that enable attacks
- Most powerful of attacks with often little chance of amelioration.



Bluetooth anyone...

- Most phones have bluetooth
- Many of the phone have it on by default
- Many of the phones are susceptible to attack
- Free tools out there to use



Network exploit

- Wireless...seriously do not use it
- ADSL modems have been compromised
- Our honeypots detect over 5000 malcodes per month these are setup to act as home ADSL accounts...

USB – Universal Stupidity Bus

- A good covert channel
- Often a lot a corporate data are left on them or stolen with them
- Come in all shapes and sizes, capacities
- In a corporate environment Windows XP Service Pack 2 turn off autorun and disable USB

Laptops, Phones, GPS

- Theft of same can tell a lot about you
- Where and when you are in the world...we are creatures of habit
- But wait why steal it when I can buy it auction...

Wetware

- The “consultant” who plugs in
- Poor process or security awareness (SE)
- Poor people management
- Net abuse/slacking



Physical Security

- Server rooms often left open
- Desktops not locked down
- Machines still logged in
- Machines not secured to desks
- Passwords on post it notes
- Swipe Cards
- Cleaners



Hardening Up

- Enable EFS and encrypt your folders, available on Win2000 +
- Truecrypt your USB memory sticks or external hard drives
- Always use VPN to connect to your office, Windows, Mac etc have it built in
- Password protect your office documents when sending them.
- Reduce your online profile

Hardening up

- If you are not using power it off – ADSL, bluetooth
- Buy restraints or strong boxes for your gear. Think the gear is often nowhere near the “cost” of what is stored on it
- If you serious about security or require high security do not use wireless.

Hardening up

- Do your updates and regularly...
- Employ some CCTV/Video in critical areas
- If you're a business think about "the net" on the desktop. Instead opt for a kiosk or "net" enabled network which is separate.

Free Stuff

Truecrypt

<http://www.truecrypt.org>

Spybot Search & Destroy

<http://www.safer-networking.com>

EFS

In your Windows2000 Pro



Summary

- Turn off Modems and Blue-tooth when not in use
- Turn on Firewalls with highest level of protection
- Do not use Wireless Networks
- Consider Disabling USB ports to protect corporate information
- Always encrypt information on USB unless it is to be made public
- Have a security policy for visitors who plug into your network [it is safer to give them a PC to use]
- Physical Security is important especially swipe-cards and access methods for cleaners
- Reduce your online profile

Contact

- <http://www.secau.org>
- c.valli@ecu.edu.au
- 93706013

