

# **Network Security Auditing**

## **Why do we Audit?**

- A mainframe may be more secure as dumb terminals won't have removable media making it harder to steal information or upload a virus. There is only a need to restrict access to the mainframe itself.
- In contrast a peer to peer network of standalone machines could be seen to be quite weak. Due to removable media, more than physical location and individual users may have admin rights.
- The IT system of a company is often seen as the most valuable part, with many companies now dependant on IT. The biggest fears are data theft, corruption, deletion and down time.

## **Who causes these problems?**

- External Hackers – Someone with no legitimate reason accessing the company's network remotely.
- Internal Hackers – Someone with no legitimate reason entering your office and accessing the company's network from company machine.
- Internal Employee – Any employee who has an axe to grind.

## **Why would an employee do this?**

- Industrial Espionage – an employee may be accessing a file and passing them on to another company.
- Malicious Acts – (deletion of files or file contents), seeking revenge as they are disgruntled with the company in some way.
- The IT Enthusiast – An employee who at home has a small Linux network set up to control everything from his video recorder to his toaster who thinks he knows how to improve the IT system.
- The average User – someone who bumbles around lost through the computer without knowing what they are doing.

## **Why Do Problems Occur?**

- Lack of day to day administration (service packs and hot fixes, etc).
- Lack of appropriate hardware/software.
- Lack of user training (people that don't know what they are doing are dangerous).

## **Identifying the Risks**

- Account names that are easy to guess correctly.
- Accounts that will have administrative properties (bypass security levels and install malware software).

## **Top 5 Passwords**

1	Password
2	123456
3	qwerty
4	abc 123
5	letmein

Passwords should include the following:

1. Uppercase (A,B,C)
2. Lowercase (a,b,c)
3. Numerical (1,2,3)
4. Objects (!,&?)
5. Some systems even require 10 characters.

*Examples:*

*Jack – very weak easy against dictionary attacks.*

*HE!Pm2y0u – Long enough, contains uppercase, lowercase symbol and numbers all in one password.*

## **Password Security**

- Ideally passwords should be easily remembered by the user whilst still offering strong protection against brutal forcing tools such as LoPhtCrack.

## **Back On Track**

- Can you see how easy it is how to get into a administrate machine when the password is 1,2,3,4,5,6.
- In windows vista the administrator account has been made into an account that you can not log into.
- In XP it is recommended that you rename the administrator account to some thing different and sent a strong password. It is possible for a hacker to re-enable accounts once they are in of course.

## **Identifying the risks**

- There is one other account that is built into Windows that is often turned on – The Guest Account.
- This is another account should be disabled and given a strong password.
- As by default the guest account was disabled system administrators didn't set password.

## **Different Hacks**

- Trojans – are a backdoor way into someone machine, they cannot replicate (like remote desktop). Well know ones are Back Orifice, Sub7, WinSpy.
- Viruses – they replicate across a single machine and other devices and set out to cause harm.
- Malware – similar to viruses' but they do not replicate.
- DOS (Denial of Service attack) – When regular pings are sent to one IP.
- Hackers can then access email, documents and even webcam's.

Viruses' can access several types of files.

- Accessing network shares.
- Bit Torrent.
- P2P sharing
- E-mail attachments.
- Drive by Downloads (you visit a site which downloads and executes codes in the background).
- When running vista or Windows 7, turning of the UAC (User Account Control) can even be expose you to attacks.

## **Fire Walls**

- To protect against attacks a product know as a firewall should be used.
- These come in the form of hardware or software products.
- Hardware firewalls are a physical box that would connect between the internet and your network.

## **Hard ware firewalls**

- They are more expensive than software.
- They are generally regarded as more secure.
- Cisco PIX firewalls are the best know ones on the market.

## **Software firewalls**

- Business firewalls are centralised applications that run on servers (examples EG ISA Server, Squid (for Linux), Novell, Microsoft Internet security and acceleration server (Microsoft).)
- Personal Firewalls – used to run on local computers, designed to prevent it from attack by intercepting packets between their arrival at the PC and reaching applications.
- Windows XP, Vista and Windows 7. This is not very good.
- Alternative Software firewalls – Zone alarm, Sygate, Norton and PC Tools.

## **What to check when doing an Audit?**

1. Firewall settings.
2. Anti-virus Software & updates
3. Passwords – Weak/Strong
4. User Accounts – Privileges/ Admin / Guest account?
5. Auto Updates – All updated.