Agenda

- Objective of The Day
- Identified The Risks
- **Who** should be involved
- **Where** To Starts
- **What** To Audit
- **When** To Audit
- **How** To Do It
Objective

- Harden Our Servers
  - In Depth Defense

- Find the loophole
  - Find the zero day
Risk

Only one risk – Human

To Err Is Human
It's our job to find it. :-)
Risks

- Not a latest Patches
- Forget my password
- Allow all, Deny None
- Install everything
- Share anything
- Phishing
- No backup
Not The Latest Patches

- Be alert
  - http://www.securityfocus.com/
  - http://packetstormsecurity.org/
  - http://gcert.mampu.gov.my/
  - http://www.cert.org/certcc.html

Internet Storm Center
- http://isc.sans.edu/

Patches Priority One
- http://www.sans.org/top-cyber-security-risks/
Lab One

- Subscribe websites to Google Reader

- http://www.kb.cert.org/vuls/
Forget My Password

- We will use easy password
- Password must = Senang nak ingat, susah nak teka.

- Don't leak the hash
- Generate MD5 hash
- Crack MD5
  - [http://isc.sans.edu/tools/reversehash.html](http://isc.sans.edu/tools/reversehash.html)
Lab Two

- Crack this
  - password
  - abc123
  - haris
  - Your own name
  - Birthday date in numbers
  - Birthday date in any format
Allow All Deny None

- Any ports outbound open
- Not proxy between LAN and Internet
- Used by BOT to attack and comm with BOSS
Lab Three

- Telnet
  - Telnet in CMD and Shell
  - Port 80 GET /index.htm HTTP/1.1 and enter twice
  - Port 25 helo and quit

- Visit this website
  - http://canyouseeme.org/
Install Everything

- To many patches
- To many services
- Only select what you want
Share Everything

- Windows Share permission “every body”
  - Don't trust your network
- Putting files in web servers
  - Google BOT nyum-nyum
Lab Four

- Google own name in PDF files
  - harisfazillah filetype:pdf
- You own IC numbers (with and without -)
  - Do this on your own
Phishing

• The most used tactic to gain password
  – Email
  – Phone
Lab Five

- Track your organisation here
  - http://www.phishtank.com/
- You will never know, you are the target.
- Defacement Archive
  - http://www.zone-h.org/archive
Break

Jom Minum
Who

- The Management
  - ICT
  - Me

Everybody need to be involved
Lab Six

- CIS Security – The Benchmark
  - http://www.cisecurity.org/
Where To Start

- Any servers that have IP address
  - Public or Internal
  - Heavy traffic websites and Email

- LAN
  - Review firewall and proxy log
  - SMTP activities
  - IRC bot activities
  - HTTP and HTTPS requests
  - Monitor network traffic
Lab Seven

- Get the bootable CD
- tcpdump
- wireshark
- Any network analysis tools
When To Do It

- A must every 6 months
- Any security warning
Contact

linuxmalaysia@gmail.com

http://green-osstools.blogspot.com/