CON KUNG-FU

Defending Yourself @ DefCon

Presented by:
Rob DeGulielmo
rdegulielmo@hotmail.com

Defcon 16 – asleep at the wheel

- Crap! Firefox is possessed!

- DNS redirection allowed for malicious code insertion on legitimate webpages

Defcon 16 – asleep at the wheel (cont.)

- Milworm.lzm in /mnt/live/memory/images
  - *Used "uselivemod" in the BT/Tools directory. Allows you to slipstream a module on the fly*
  - *Automatic IP and calls update milworm*

Defcon 16 – asleep at the wheel (cont.)

- **MBR rootkit**
  - *Vmlinuz (compressed kernel) files were replaced with replicas to subvert grub, etc.*
  - *Try loading BT w/ nohdd, causes reboot; perhaps because the MBR rootkit depended on virtual memory created on the hdd*

What you *should* have done

- Left your laptop at home!

What you *should* have done

- Broadband wireless card
- Updates/Patches
- Laptop w/no data on it
  - *NOT your work laptop!!*
  - *NOT your home laptop!!*
- Use VM

What you can do now

- Lock down BIOS/MBR
  - *Enable system password protection*
  - *Enable MBR protection within bios. This makes MBR read-only*

What you can do now

- *Configuration changes (linux/win)*
  - Hosts.deny
  - Firewall
  - Close services
  - Change default root p/w (i.e. BT)
  - AV
  - Conky
  - Hardset DNS servers

What you can do now

- *Comprehensive Hardening*
- Security templates (windows)
- Bastille (linux) (http://bastille-linux.sourceforge.net/)
- HIPS
- Block all inbound connections
- *Protect your DNS entries/ARP/logs*

What you can do now

- *SSH Proxy*
  - Firefox tunneling over SSH
  - Know your server's SSH key beforehand!!

What you can do now

- *Firefox hardening*
  - NoScript
  - Turn off dns proxy in about:config
  - Use a known good proxy

What you can do now

- *Run Snort*
  - Patch Snort!
  - Will detect wireless shenanigans
- *Run Kismet (Linux)*
- will alert on deauthflood, bcastdiscon (disassoc. Attack)
  - http://www.informit.com/guides/content.aspx?g=security&seqNum=148
- *Run AirSnare (Windows)*

What you can do now

- *Do NOT check email, go to LinkedIn, Facebook, etc.*
  - *Even after SSL login page, many sessions are cleartext*

How to tell if you just got p0wnd

- Logs
- MD5 hashes
  - *Check system binaries (telnet, ls, login, finger, etc) against known checksums…check offline in single user mode.*

How to tell if you just got p0wnd

- Forensic Utils (Backtrack, etc)
- Connections monitor
- Monitor /etc/services as well as /etc/ined.conf

How to tell if you just got p0wnd

- Portscan detection
  - p.283 nMap Network Scanning (Fyodor)
- *Scanlogd*
- *PortSentry*
- *ZoneAlarm (windows)*
- *Psad (Linux): Intrusion Detection and Log Analysis with iptables*
  - http://www.cipherdyne.org/psad/

Strike Back !

It's the most hostile network in the world

Be part of it!

Strike Back !

- Tools at ready to terminate access or impart retribution
- Run windentd & icepick
  - (p.264 nMap Network Scanning)
- Scanlogd
- PortSentry
- Targeted DOS
  - Please do not DOS the DC network….that is very bad form, and bad things ™ will happen…too you