

Threats from the Malicious Insiders

Adli Abdul Wahid

adli@kict.iiu.edu.my

<http://kict.iiu.edu.my/adli>

Dept. of CS,
Kulliyah of ICT
International Islamic University Malaysia

Agenda

- Perimeter Defense
- Sources of Threats
- Internal Network != Secure Network
- Attacks
- Who's responsibility
- Conclusion

Perimeter Defense

- Defense focuses on mitigating attacks at the perimeter
 - Firewall, Intrusion Detection Systems
 - Rules are tight on connection from external
- System administrator pay attention to servers on the DMZ or certain segments
 - But who's watching the rest of the PCs monitoring activities in the internal networks ?

Source of Threats

- Attacks from external
 - Not part of the organization
 - Have limited targets to begin with (servers on DMZ)
 - Need to overcome several 'layers' of defence
- Attacks from inside
 - Knowledge the organization well – people, place, targets
 - Access to more than just boxes in the DMZ
 - Additional resources (time, bandwidth)

Scope and Targets

- Scope
 - Large
 - What is visible from one's point of view
- Targets
 - Firewall, Router, Switches
 - {Database, Web, Email, DNS} Servers
 - PCs
 - Contains documents, applications etc.
 - Printers

Scope & Targets (2)

- With inside information, easier to zoom in on target
 - What is the CFOs IP address
 - Where is the administrator's VLAN
 - Who's notebook contains company's secret

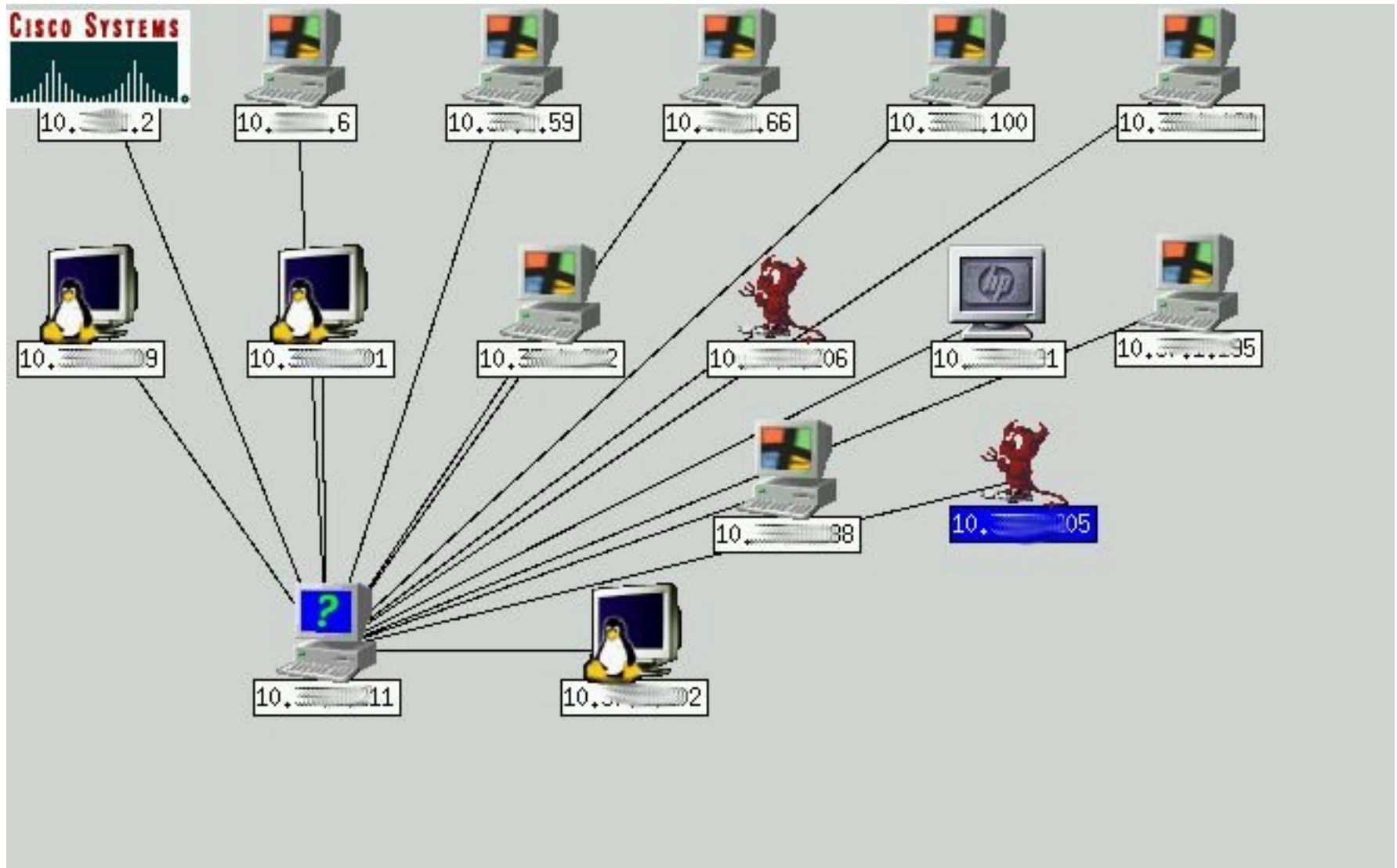
Techniques

- Information Gathering
 - OS Fingerprinting, Host enumeration , Port Scanning
 - Network Monitoring
 - Social engineering
- Aggressive attacks
 - Sniffing (for passwords)
 - Compromising by exploiting vulnerabilities
 - Denial of Service
 - Physical attacks (arson, theft)

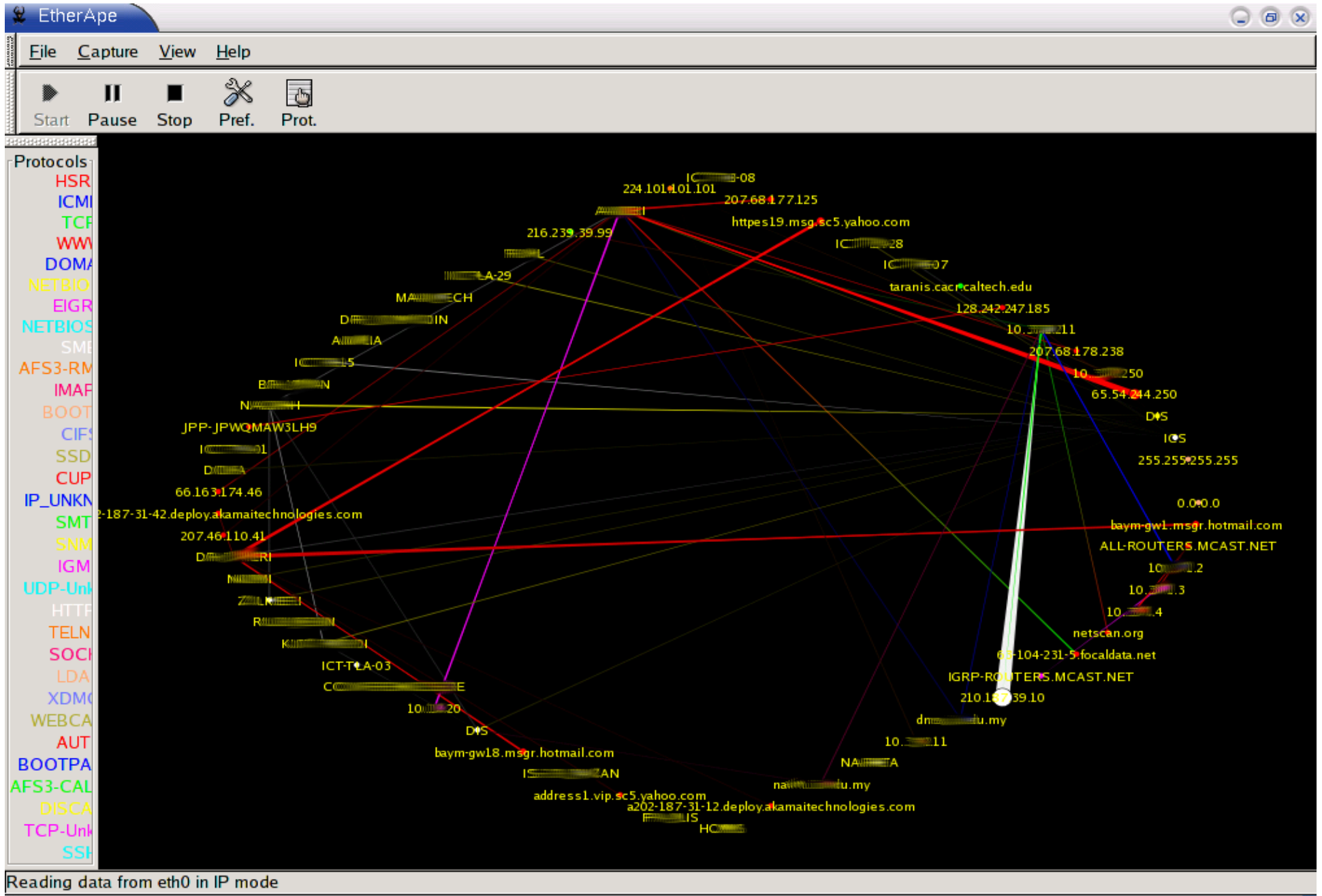
Tools are abundant

- Password Sniffing
 - Dsniff, Ettercap
- Vulnerability assessment
 - Nessus
- Network/Port Scanners
 - Nmap, xprobe2, nbtscan, cheops-ng
- Attacking
 - Publicly available exploits
 - Metasploit Framework

Cheops-NG Output



Monitoring network activities with Etherape



Web Managing the WAP

D-Link DWL-1000AP Management (version 1.0.0) - Konqueror

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://10.0.0.1:8080/framework/base.shtml

MandrakeSoft MandrakeStore MandrakeExpert MandrakeSoft News Software Programming Window Manager ftp://ftp.stealth

D-Link D-Link Wireless Access Point DWL-1000AP

DEVICE INFORMATION

Settings Summary

CONFIGURATION

Wireless Settings

SECURITY

Access Control List (Security Against Unauthorized Network Access)

WEP Encryption (Security Against Eavesdropping)

WEP Encryption

Open System (No Authentication)

WEP [Change Settings](#)

Cancel Apply

On this page you can enable or disable

- Open System: wireless clients do not require authentication.
- WEP: wireless clients must enter a key to access the network.

WEP (Wired Equivalent Privacy) requires the use of WEP keys. For 64-bit WEP encryption, the password is 10 hexadecimal characters (from '0' to '9', 'A' to 'F'). For 128-bit WEP encryption, the password is 26 hexadecimal characters. To configure WEP.

Enter the WEP Settings

WEP security requires selection of a WEP mode and key.

Security method:

WEP 64-bits (10 characters separated with colon eg. 01:26:xx)

WEP 128-bits (26 characters separated with colon eg. 01:26:xx)

Type new WEP Key:

OK Cancel

Telnet Session !

```
10.x.y.z.3356 > 10.a.b.c.23: P 1113789614:1113789615(1) ack 2525581217 win 16096 (DF)
10.x.y.z.3356 > 10.a.b.c.23: . ack 2525581218 win 16095 (DF)
10.x.y.z.3356 > 10.a.b.c.23: P 1113789615:1113789616(1) ack 2525581218 win 16095 (DF)
10.x.y.z.3356 > 10.a.b.c.23: P 1113789616:1113789617(1) ack 2525581219 win 16094 (DF)
```

Dsniff captures password

```
06/13/05 16:52:23 tcp 10.x.y.z -> 10.a.b.c (telnet)
passwd
en
passwd.123
```


It all boils down to ..

- Is the security mechanism in place to:
 - Detect scanning/sniffing attempt from 1 PC to another in within a VLAN
 - Check PCs that has not been patched / or upgraded with the latest security fix
 - Detect if one of the core switches have been compromised
 - Check if users are using simple passwords for their (pc/email/etc) accounts

Conclusion

- Attacks come from external and inside
- Insiders have a certain level of advantage to mount a successful attack
- Security administrators need to place sufficient security controls to mitigate attacks from external and internal
 - Good perimeter defense + network security monitoring

end()

adli@kict.iiu.edu.my