"Cheap Security Audits with Linux LiveCDs"

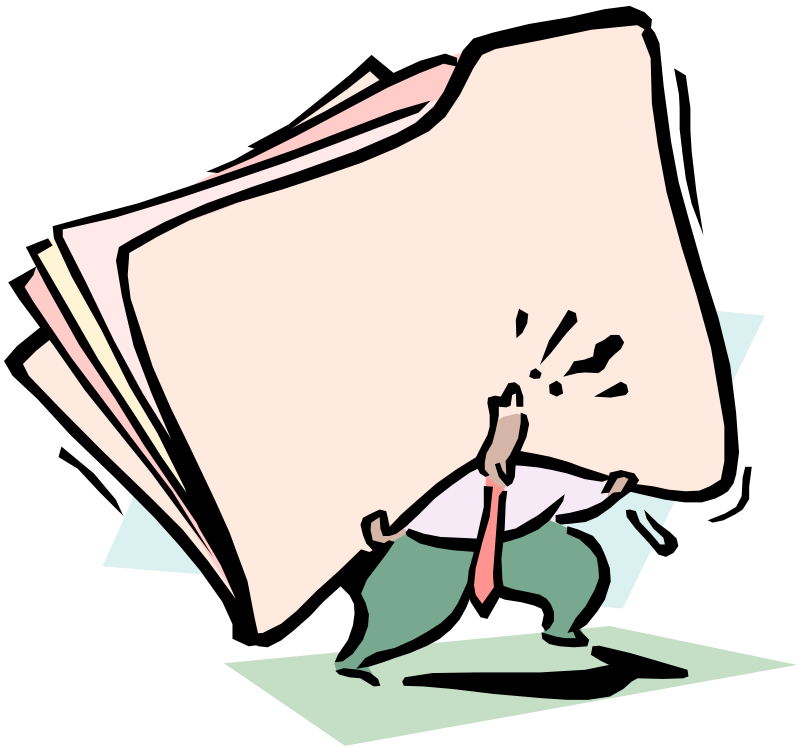
Presented by Beth Lynn Eicher

bethlynn@cs.cmu.edu

For Western PA Linux Users' Group and Pittsburgh SAGE

8/13/2005

You might be a system administrator if…



- Your friends and immediate family call you when their computer crashes
- You are the sole IT person in your organization
- Your boss asks you to fix computers on a consistent basis

What do we mean by “cheap”

- Not going to cost you any $
- Maybe not the best way to do this, monitoring systems are better (snort and tripwire)
- It’s not going to cost you very much time.

What exactly do we mean by “audit”

- To observe the current conditions and document
- We are not attempting to crack - or to test the strength by trying to intrude
- Auditing is not to be confused with monitoring

Recommended Linux CDs

- Knoppix
- Knoppix-STD
- WHAX - formerly known as Whoppix

- Burn chkrootkit and rkhunter
  - Check for rootkits and trojans

Users will not ask for a security audit

- If it’s not broke, why fix it?
- What could possibly go wrong?
- Why are you invading my privacy?
- Don’t you trust us?

Management is not likely to ask for a security audit either, however …

- You may need to do so to comply to legal, customer, or partner standards
- A security incident may get management to pay attention
- Check occasionally for IT policy compliancy
- Protect a specific mission-critical resource
- Vulnerability+exposure=liability

You need to initiate this process

You must get management approval first

Now is not the time to take Grace Murray Hopper's advice, "It is much easier to apologize than to ask permission."

Why?

- Proceeding without permission could be illegal.
  - PA Title 18, Chapter 76: Computer Offenses
- You could accidentally create a denial of service as you are auditing
- If an attack, accident, or disaster coincidentally occurs, you do not want to be blamed.
- Unless you already have a published policy that security audits will be done unannounced, you are invading your user's privacy
- You should strive to the SAGE ethics code http://www.sage.org/ethics.mm

How?

- Document the entire scope and get management to sign-off
  - What systems will be audited
  - What tools you will use
  - When you are doing this
  - If you find something, are you allowed to further investigate?

Scenario #1

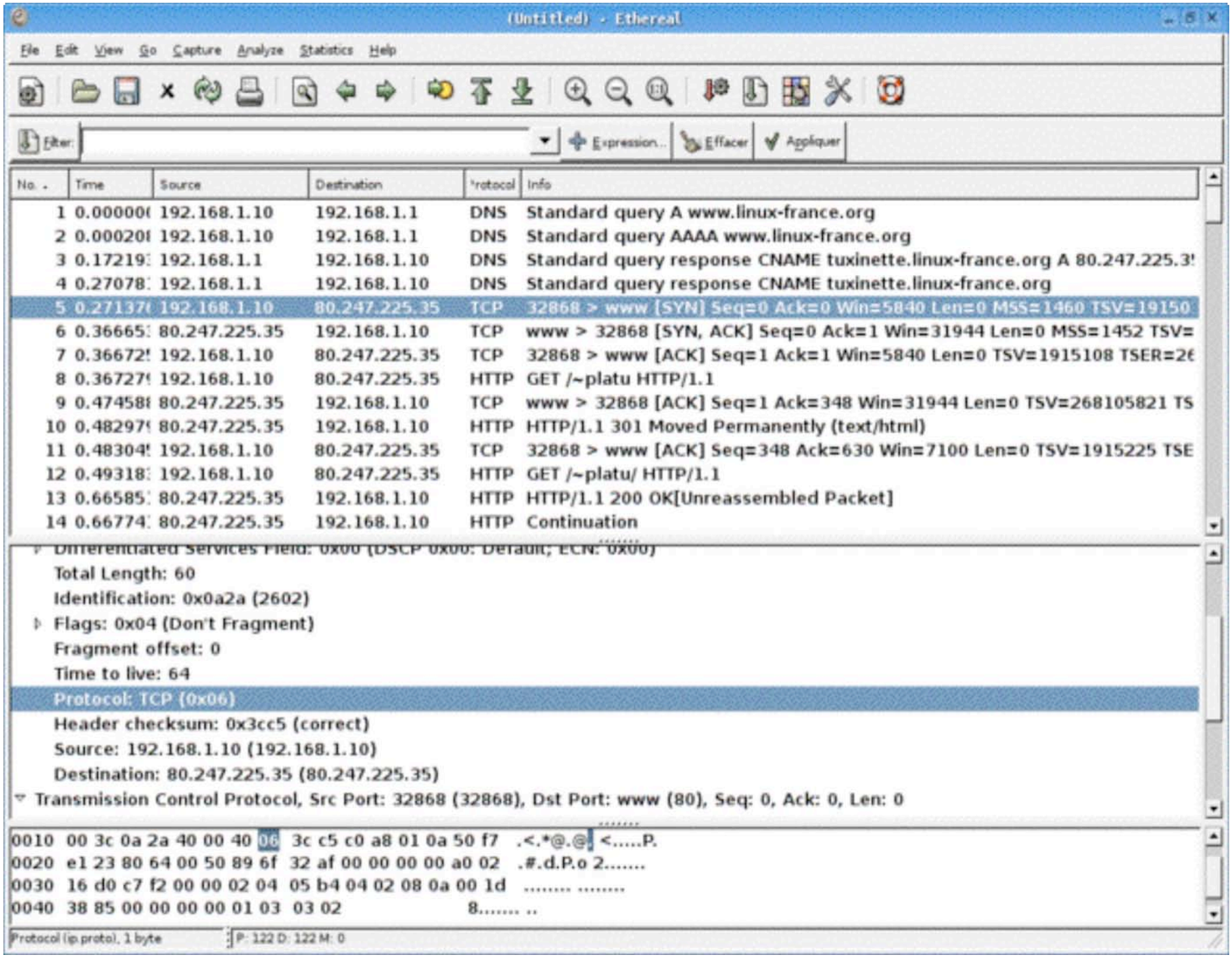
You have been recently hired by a small company to be the sole IT person. Nothing has been documented so no one knows what each computer does.

The risks

- No one admits to knowing the passwords
- There are several neglected systems that could already be exploited
- In the meantime, the users are typing their passwords on these neglected systems

How to do the audit

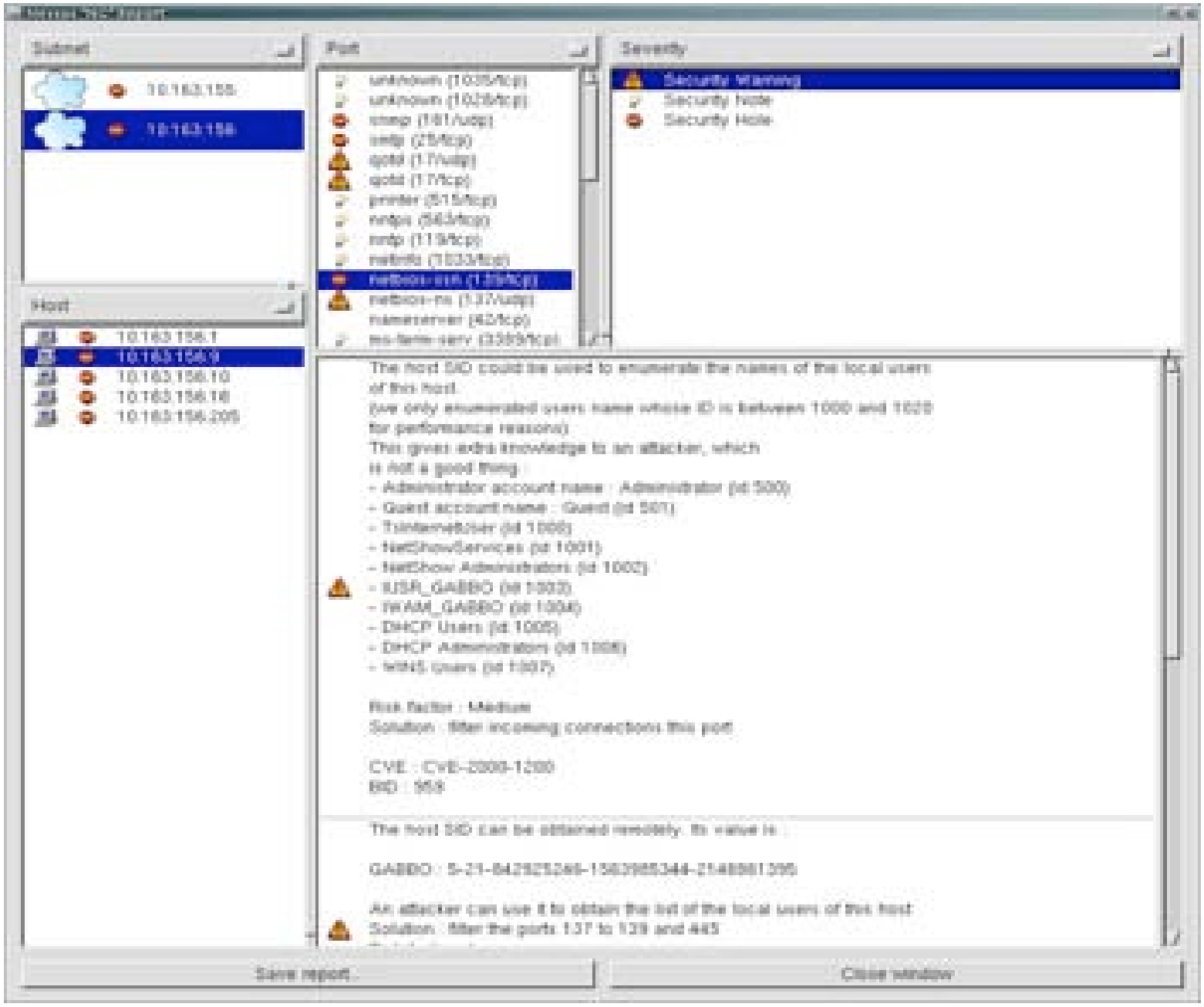
- Boot Knoppix-STD off of the CD
- Use ethereal to capture packets for a few days and use nmap to document open ports and follow up with Nessus
- You should look for
  - Identify the ip address of each system on your network
  - What services are running
  - Watch for remote logins


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Effacer
Appliquer
No. Time Source Destination Protocol Info
1 0.00000(192.168.1.10 192.168.1.1 DNS Standard query A www.linux-france.org
2 0.00020(192.168.1.10 192.168.1.1 DNS Standard query AAAA www.linux-france.org
3 0.17219: 192.168.1.1 192.168.1.10 DNS Standard query response CNAME tuxinette.linux-france.org A 80.247.225.3
4 0.27078: 192.168.1.1 192.168.1.10 DNS Standard query response CNAME tuxinette.linux-france.org
5 0.27137(192.168.1.10 80.247.225.35 TCP 32868 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 TSV=19150
6 0.36665: 80.247.225.35 192.168.1.10 TCP www > 32868 [SYN, ACK] Seq=0 Ack=1 Win=31944 Len=0 MSS=1452 TSV=
7 0.36672! 192.168.1.10 80.247.225.35 TCP 32868 > www [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=1915108 TSER=2(
8 0.36727! 192.168.1.10 80.247.225.35 HTTP GET /~platu HTTP/1.1
9 0.47458(80.247.225.35 192.168.1.10 TCP www > 32868 [ACK] Seq=1 Ack=348 Win=31944 Len=0 TSV=268105821 TS
10 0.48297! 80.247.225.35 192.168.1.10 HTTP HTTP/1.1 301 Moved Permanently (text/html)
11 0.48304! 192.168.1.10 80.247.225.35 TCP 32868 > www [ACK] Seq=348 Ack=630 Win=7100 Len=0 TSV=1915225 TSE
12 0.49318: 192.168.1.10 80.247.225.35 HTTP GET /~platu/ HTTP/1.1
13 0.66585: 80.247.225.35 192.168.1.10 HTTP HTTP/1.1 200 OK[Unreassembled Packet]
14 0.66774: 80.247.225.35 192.168.1.10 HTTP Continuation
Total Length: 60
Identification: 0x0a2a (2602)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x3cc5 (correct)
Source: 192.168.1.10 (192.168.1.10)
Destination: 80.247.225.35 (80.247.225.35)
Transmission Control Protocol, Src Port: 32868 (32868), Dst Port: www (80), Seq: 0, Ack: 0, Len: 0
0010 00 3c 0a 2a 40 00 40 06 3c c5 c0 a8 01 0a 50 f7 .<.*@.@. <.....P.
0020 e1 23 80 64 00 50 89 6f 32 af 00 00 00 00 a0 02 .#.d.P.o 2.....
0030 16 d0 c7 f2 00 00 02 04 05 b4 04 02 08 0a 00 1d ....
0040 38 85 00 00 00 00 01 03 03 02 8..... ..
Protocol (ip.proto), 1 byte
P: 122 D: 122 M: 0

```
[root@OPSEC /root]# nmap -sT -v -v 10.18.1.148

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host opsec.suffolk.edu (10.18.1.148) appears to be up ... good.
Initiating TCP connect() scan against opsec.suffolk.edu (10.18.1.148)
Adding TCP port 1024 (state open).
Adding TCP port 443 (state open).
Adding TCP port 6000 (state open).
Adding TCP port 80 (state open).
Adding TCP port 22 (state open).
The TCP connect scan took 1 second to scan 1523 ports.
Interesting ports on opsec.suffolk.edu (10.18.1.148):
(The 1518 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
80/tcp     open        http
443/tcp    open        https
1024/tcp   open        kdm
6000/tcp   open        X11

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
[root@OPSEC /root]#
```


Subnet
10.163.155
10.163.156
Host
10.163.156.1
10.163.156.9
10.163.156.10
10.163.156.18
10.163.156.205
Port
unknown (1035/tcp)
unknown (1026/tcp)
snmp (161/udp)
smtp (25/tcp)
qotd (17/udp)
qotd (17/tcp)
printer (515/tcp)
nntps (563/tcp)
nntp (119/tcp)
netinfo (1033/tcp)
netbios-ssn (139/tcp)
netbios-ns (137/udp)
nameserver (42/tcp)
ms-term-serv (3389/tcp)
Severity
Security Warning
Security Note
Security Hole
The host SID could be used to enumerate the names of the local users
of this host.
(we only enumerated users name whose ID is between 1000 and 1020
for performance reasons)
This gives extra knowledge to an attacker, which
is not a good thing :
- Administrator account name : Administrator (id 500)
- Guest account name : Guest (id 501)
- TsInternetUser (id 1000)
- NetShowServices (id 1001)
- NetShow Administrators (id 1002)
- IUSR_GABBO (id 1003)
- IWAM_GABBO (id 1004)
- DHCP Users (id 1005)
- DHCP Administrators (id 1006)
- WINS Users (id 1007)
Risk factor : Medium
Solution : filter incoming connections this port
CVE : CVE-2000-1200
BID : 959
The host SID can be obtained remotely. Its value is :
GABBO : S-21-842825249-1563985344-2148861395
An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139 and 445
Save report...
Close window

One quick fix

- Change all the root passwords on the Linux/Unix systems by booting into single user mode
- chntpw on Knoppix-STD can help you change Windows passwords

Scenario #2

You notice an usually large amounts of bandwidth usage coming from an ip address that belongs to a Linux desktop.

The risks

- Someone could have stolen the ip address and your bandwidth
- The user could be abusing resources by downloading or sharing software or media files which may be pirated
- The system may have been cracked and the cracker and his friends may be stealing your bandwidth

How to do the audit

- Boot Knoppix on another system and run ethereal to log the traffic.
- Make a note of the mac address that is using the ip address in question
- If you can safely remotely login, then use ps, lsof, and top to see what's going on. Also verify the mac address with ifconfig
- Run chkrootkit and rkhunter

Scenario #3

Your employer recently implemented a policy of stronger passwords and you have been asked to check for compliance.

The risks

Weak passwords can lead to internal and external cracking.

How to do the audit

Knoppix-STD has password crackers

- John the Ripper for Linux/Unix /etc/shadow files
- Pwl9x for windows password files

Sorry, that’s all folks

Special Thanks to…

- Hosts today - Bill Moran, David Ostroske, and Esther Filderman
- USENIX, SAGE, and SIA