



TENABLE

Network Security[®]

KEEPING UP WITH THE JONES'S FORENSICS

- **IT security forensics technologies**
 - Not focused on disk encryption or biometrics
 - Not focused on procedure, chain of custody, integrity of data, .etc
- **Review what they DO and DON'T track**
- **Review their impact on compliance**
- **Will do this through comparison of two fake companies:**



Take Aways

- No technology is perfect
- Many are complementary
- Many can be abused

Intro - Who Am I?

- **CTO of Tenable Network Security**
 - Makes innovative vulnerability detection and security event management tools
 - Develops and supports the Nessus vulnerability scanner project
 - Works with lots of MSPs and customers
- **Enterasys Networks/NSW**
 - Wrote original Dragon IDS
 - Worked with lots of MSPs and customers
- **Was in your shoes ...**
 - Ran vulnerability and IDS teams for an ASP
 - Helped plan large-scale security for a telco
 - Did security research and pen testing at NSA



Introduction – Who is Tenable?

- **We run the Nessus project**
 - More than 85,000 organizations world-wide
 - We develop 99.9% of the plugins
 - Develop and test all of Nessus 3
 - The **Direct Feed** subscription includes advanced configuration auditing features
- **Unified Security Monitoring**
 - Vulnerability Management
 - Compliance Monitoring & Reporting
 - Security Event Management
 - Network Behavioral Anomaly Detection
 - Passive and Active Asset discovery
 - More than 750 enterprise customers



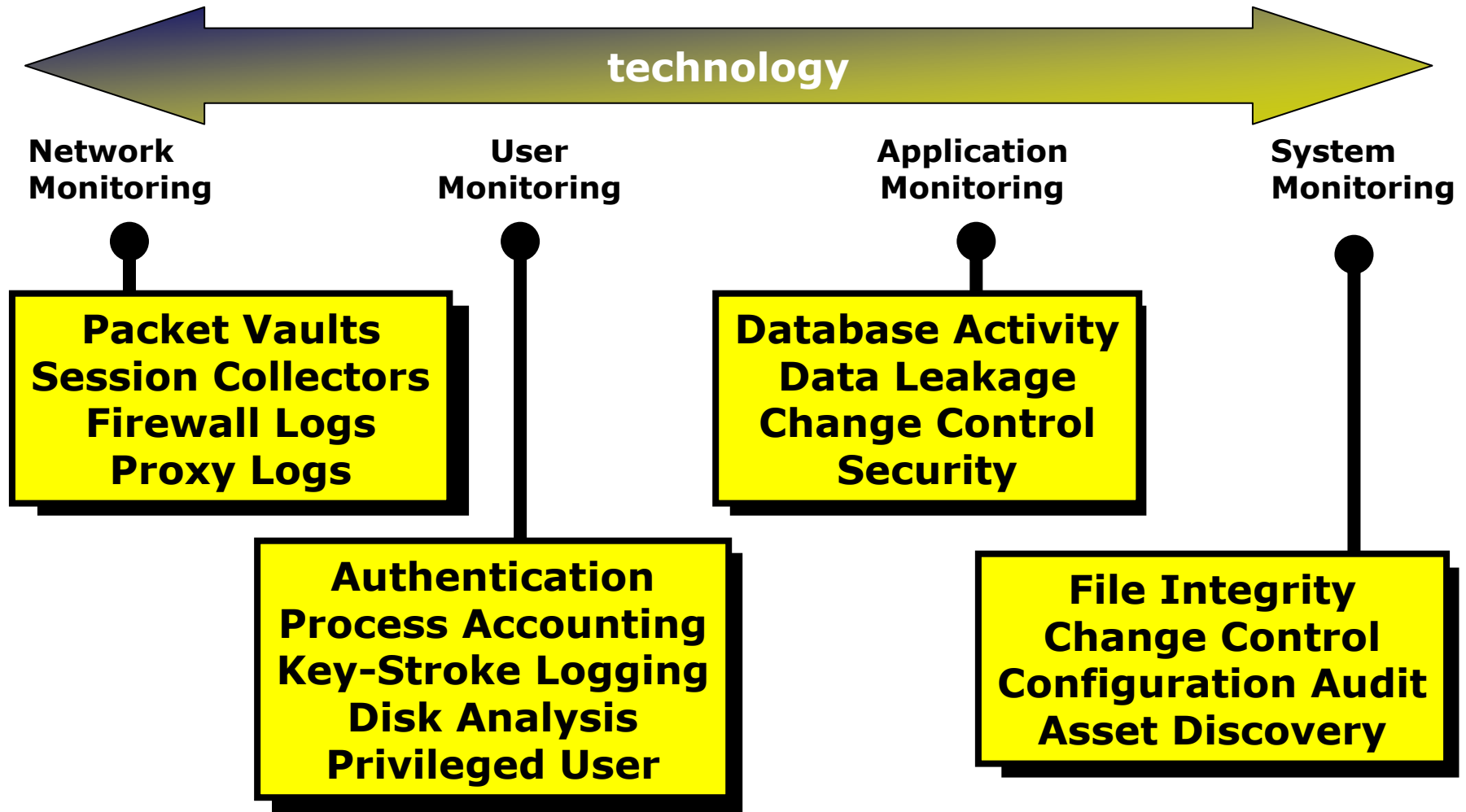
Why Do We Need Forensics?

- People are evil
- People are stupid
- Sometimes the evil people and the stupid people gang up on you
- People are not good witnesses
 - Lawyers may not believe the people as much as the computers the people set up

Why Do We Need Forensics?

- Networks are complex
- Applications are multiple system entities
- Virtualization means your systems, applications and data is just “in the cloud”

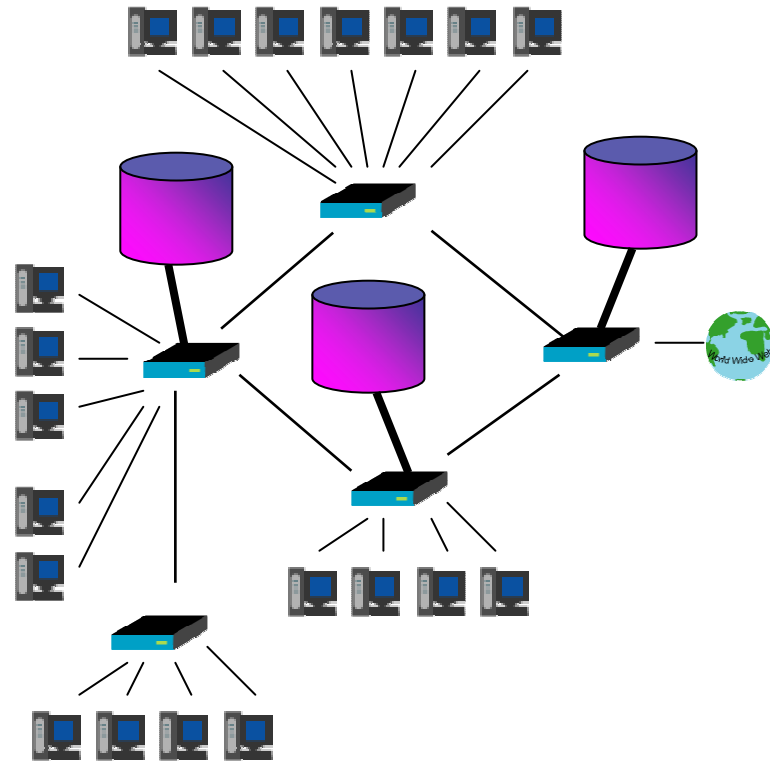
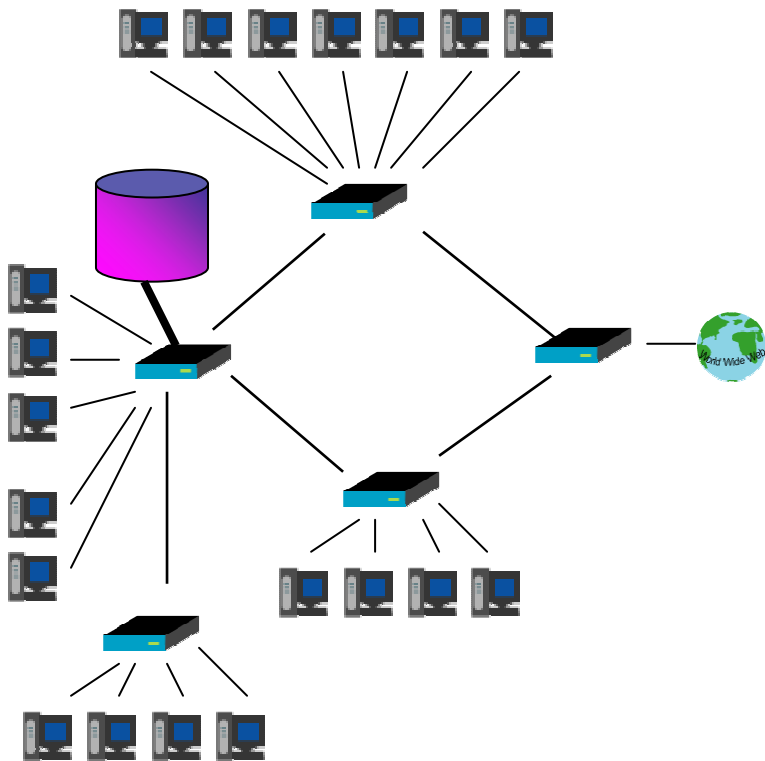
Where can we track data and activity?



Packet Vaulting

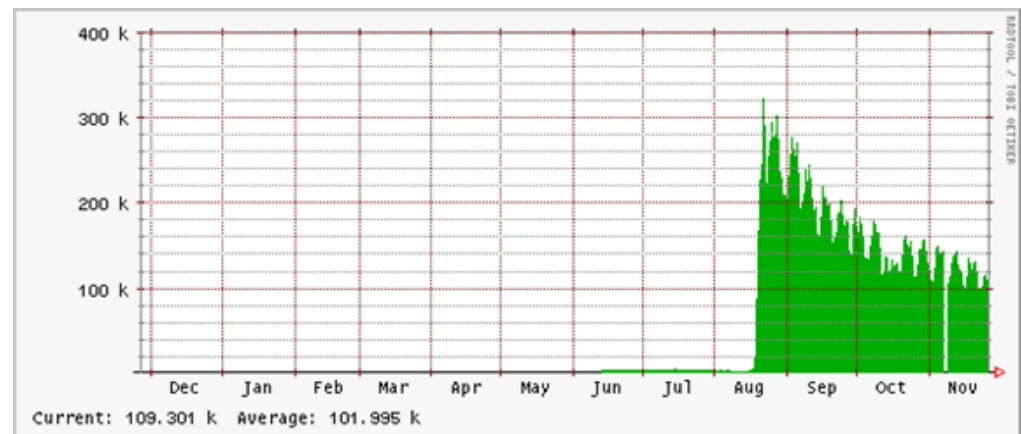
- Collect and save all (or some) of the packets
- How long can we store data?
- What can I do with the data?
 - How do you know what to look for?
- What about encryption, new protocols, tor, .etc?

Packet Vaulting

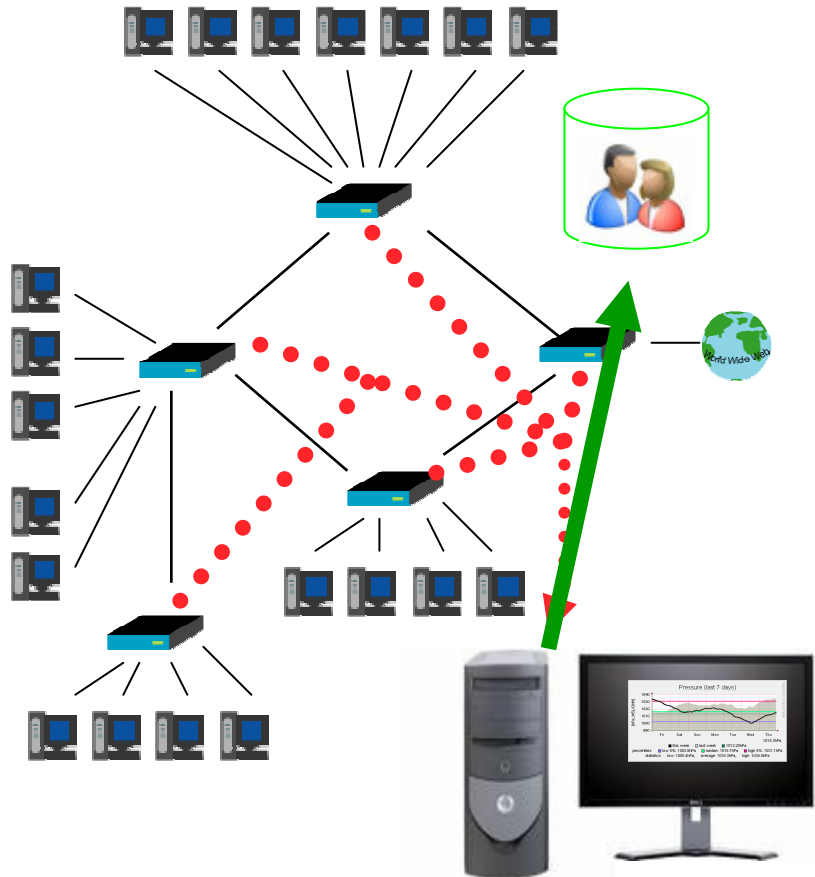
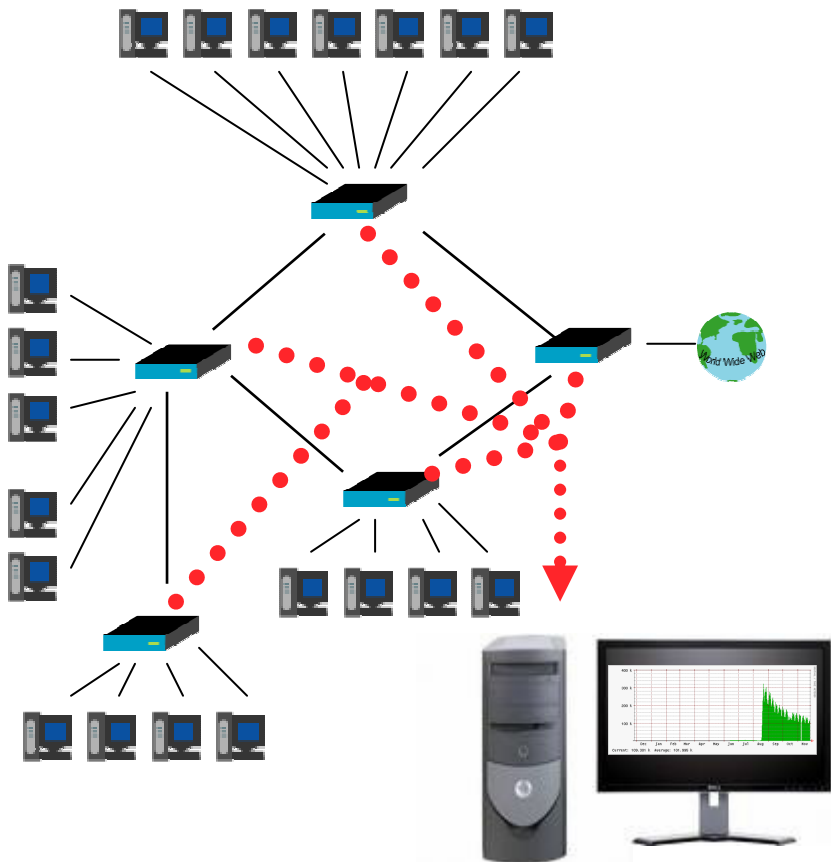


Session Collectors

- Collect and save all (or some) of the network sessions
 - Netflow & Sniffed TCP sessions
- How long can we store data?
- What can I do with the data?
- What about encryption, new protocols, tor, .etc?



Session Collectors



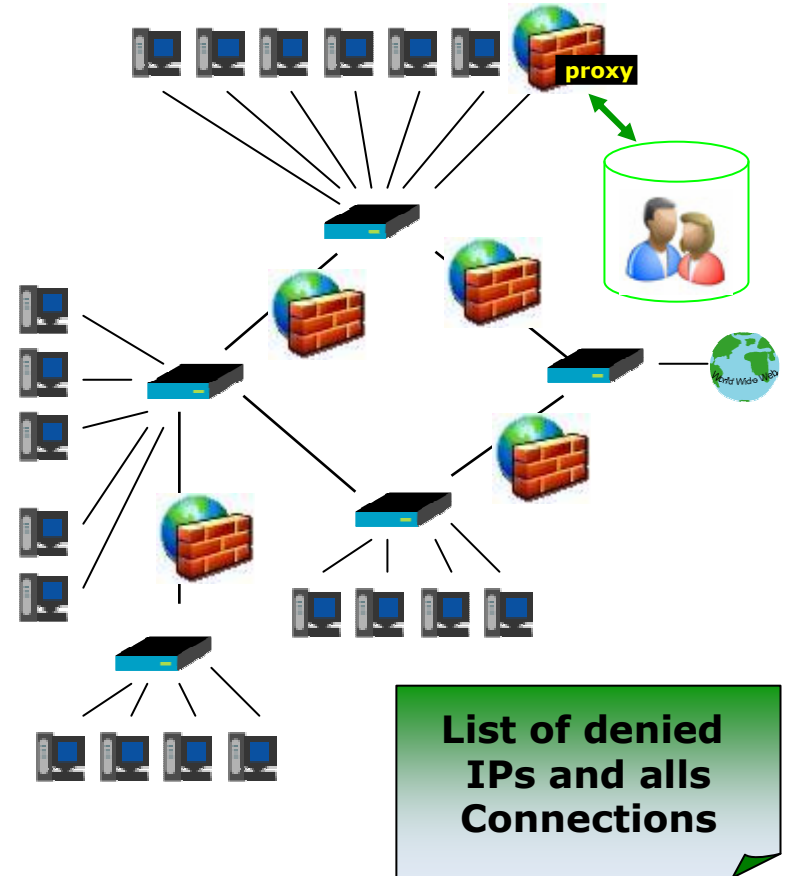
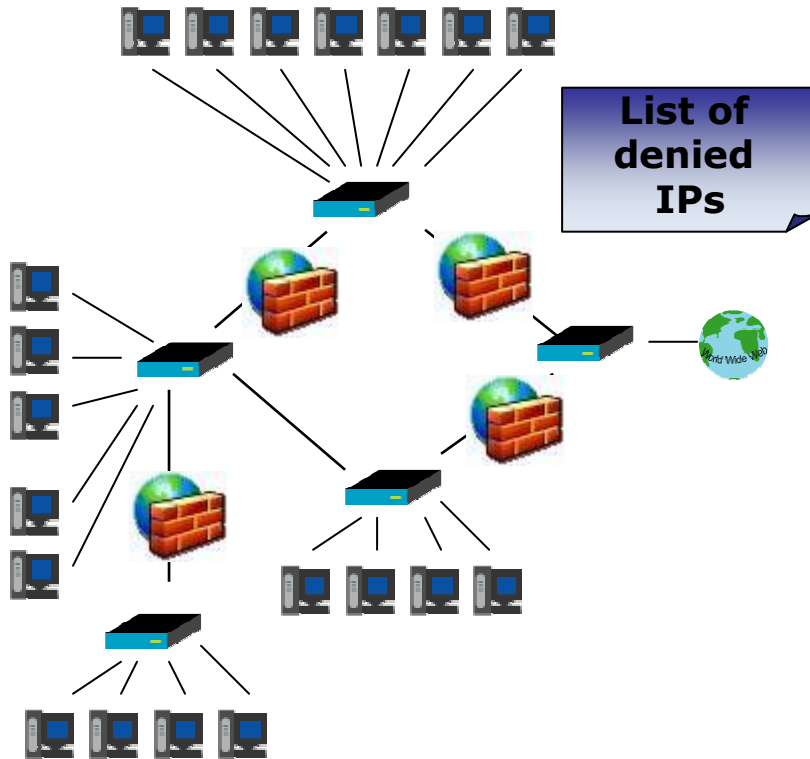
Firewall & Proxy Logs

- Firewalls and proxies are not just policy enforcement
- Firewalls block access to and from specific IP addresses to other IP addresses and ports
- A proxy actually terminates a session and initiates a re-connect to the external desired service

Firewall & Proxy Logs

- Firewalls can log ALLOWED connections in addition to DENIED connections
- For some protocols (web and smtp), it is easier to log and enforce policy with a proxy

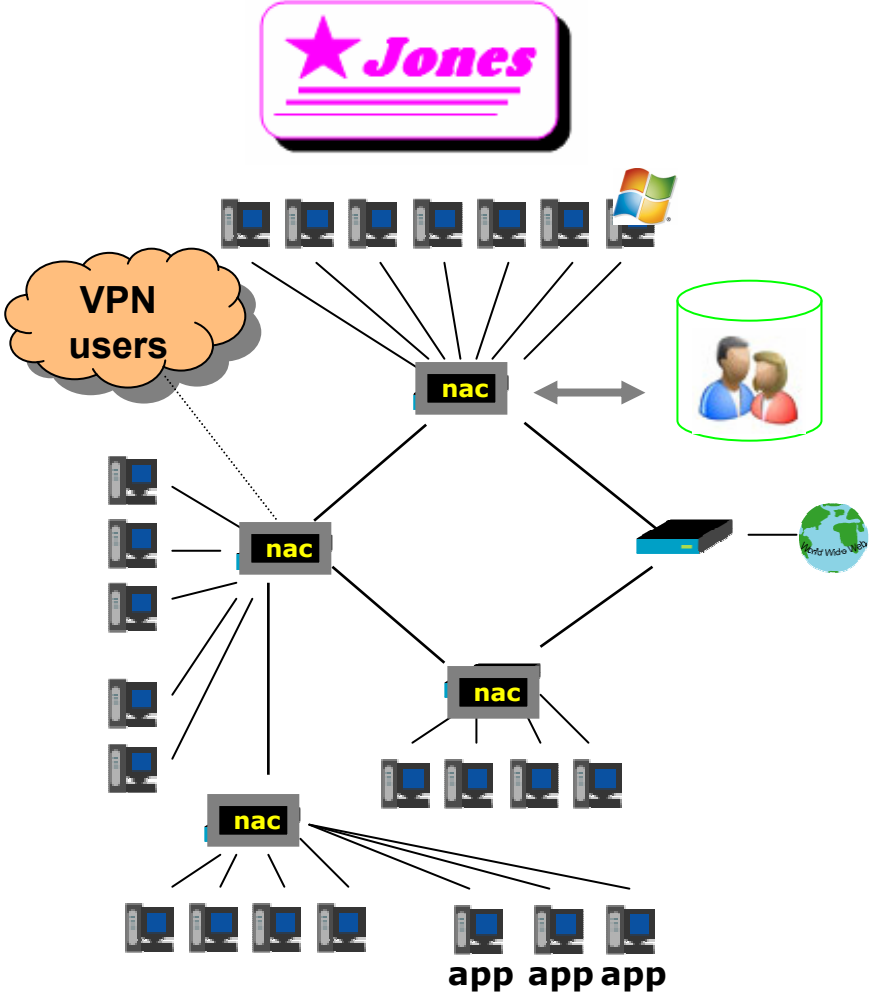
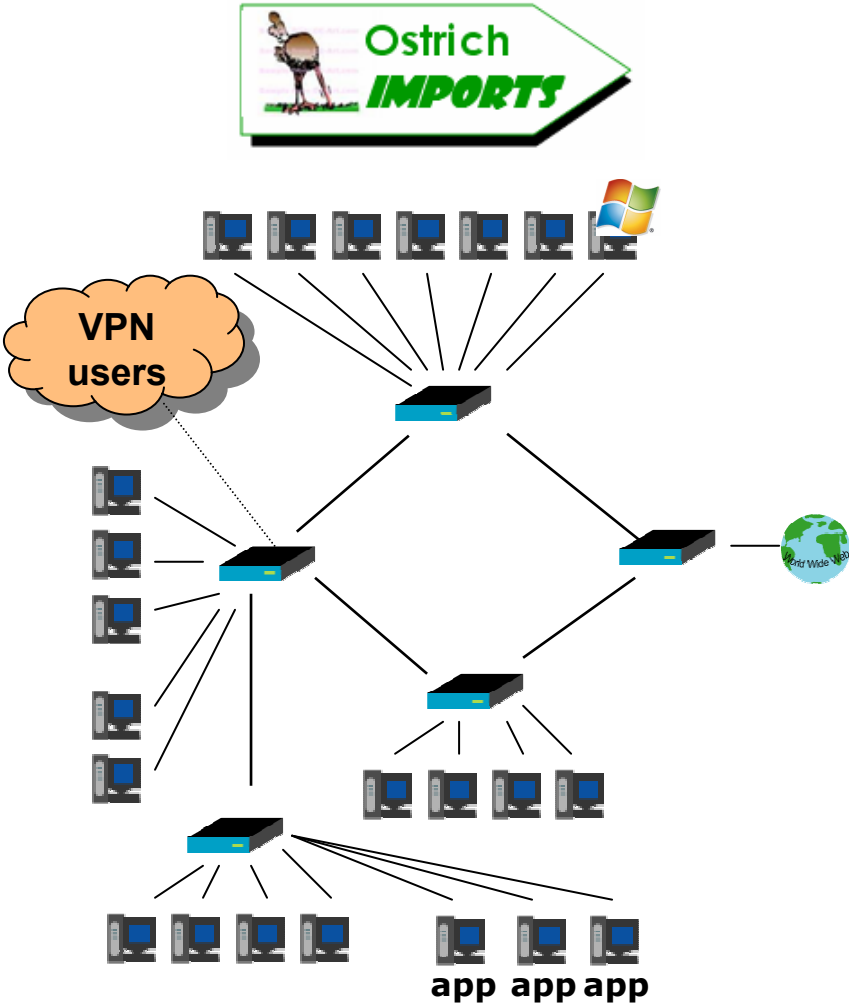
Firewalls and Proxies



Authentication

- Where do you authenticate users?
 - After they've plugged in?
 - When they log into the Domain?
 - Before they connect to the Internet?
- Are these AAA logs centralized?

Authentication



Process Accounting

- Log EVERYTHING a user does on a server
 - All files edited
 - All programs run
 - Available on Linux, Solaris, AIX, Windows, .etc
- Generates a huge audit trail
 - Requires (mostly commercial) tools to make sense of the logs
 - Can report on all activities for user “foo”
- Does have performance impact
- Not that effective for host/desktop

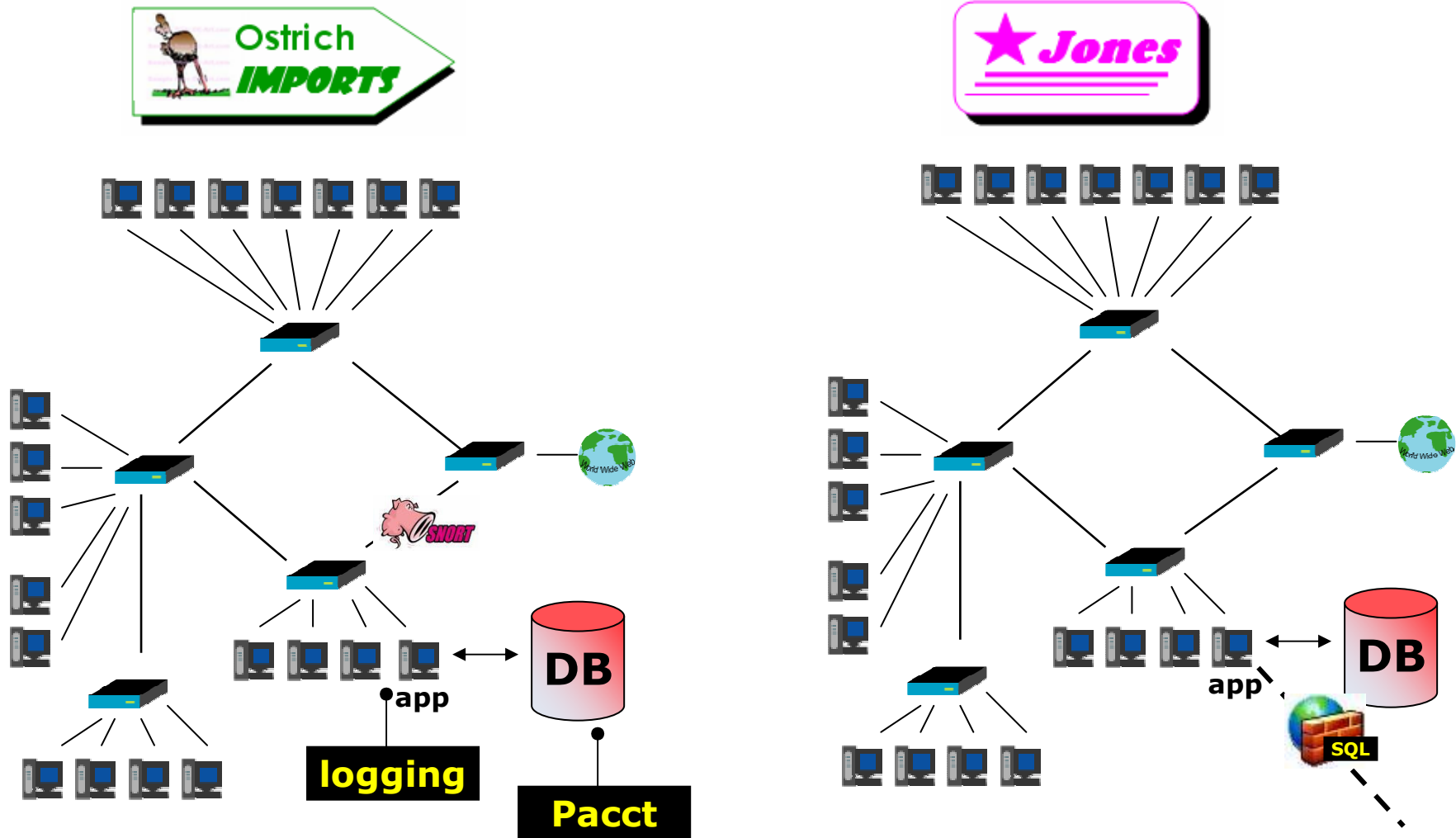
System Agents

- Log all keystrokes at desktop computers
- Be able to grab any file image and look for
 - Pornography
 - Stenography
 - Sensitive Data
 - IP and Copyright infringement
- Grab screen shots of desktops
- This is YAA
 - If you don't have corporate buy-in, your IT staff will shoot you

Database Activity Monitoring

- Logs all access to the database
 - Typically, the only way into a database is to interact with it via SQL, or to manually edit tables
- Log all inserts and queries
 - Want to be able to audit all queries
 - Want to be able to see successful SQL injection and data leakage events from the outside
 - Want to also see Joe in accounting connect via SQL and dump the customer contact info

Database Activity Monitoring

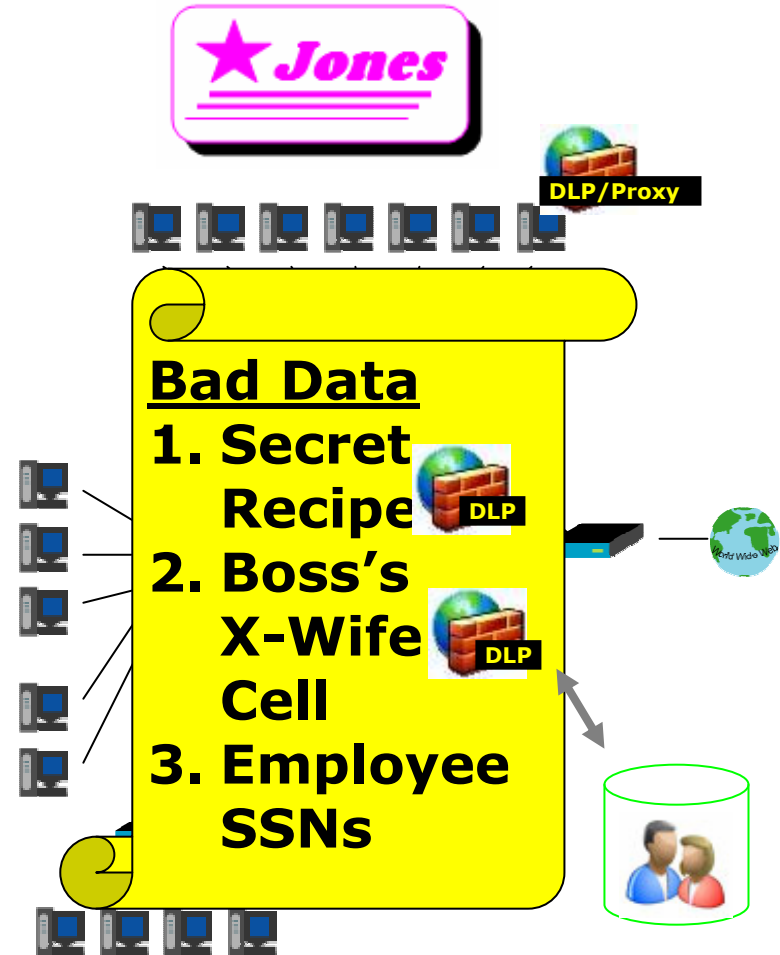
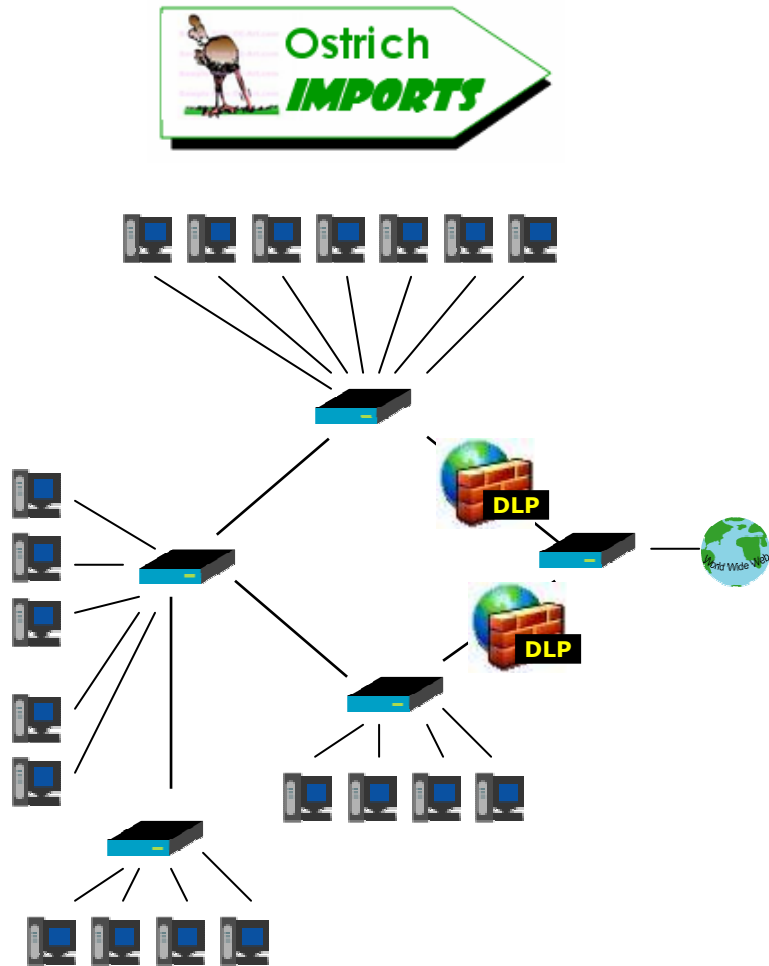


- Want to collect evidence of our users sending sensitive data when they should not be
- What is sensitive data?
- What are the use cases for sending data to 3rd parties?

Data Leakage Technology

- Agent based
 - Searches your computer for BAD data
 - Prevents you from doing anything with the BAD data
- Network Based
 - Email gateway
 - Web Proxy
 - Inline network device
- Protocols
 - SMTP, FTP, P2P, AIM, Skype, HTTP, HTTPS, .etc

Data Leakage



File Integrity Checkers

- User mathematics to compute a secure checksum
 - If the contents of the file change, then the checksum changes
- Issues
 - If system files (like executables or libraries) change, then it is a hacker, system update or reboot or whatever ...
 - If documents change, then someone edited content

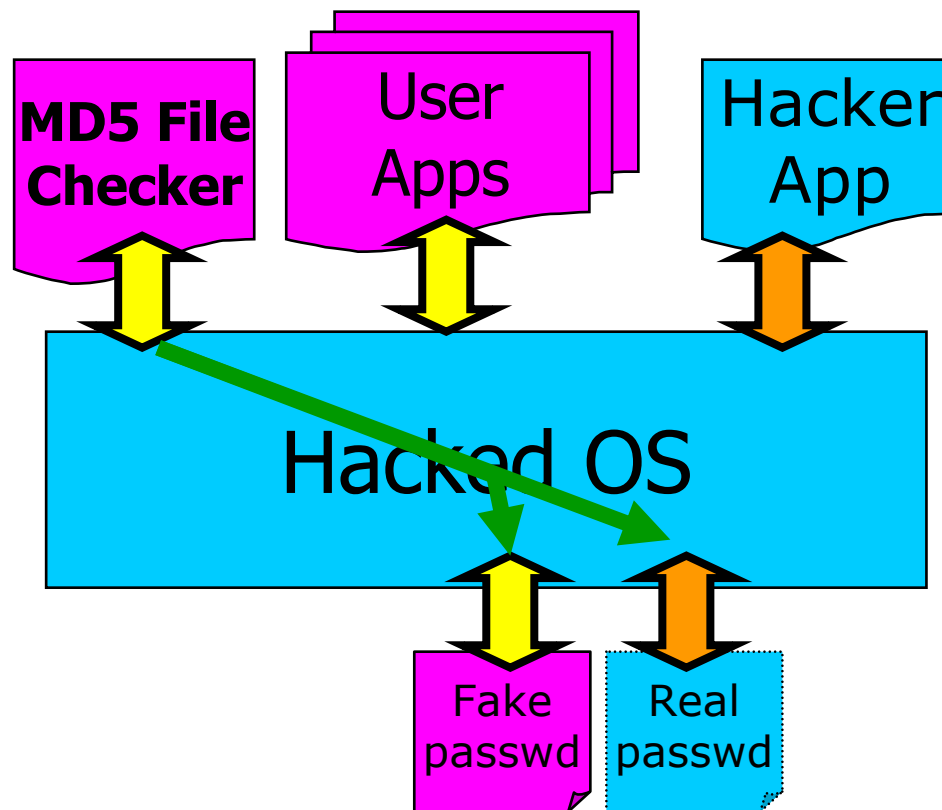
Integrity of File Integrity Checkers

```
root:*:0:0:Charlie &:/root:/bin/csh
daemon:*:1:1:The devil himself:/root:/sbin/nologin
operator:*:2:5:System &/operator:/sbin/nologin
bin:*:3:7:Binaries Commands and Source,,,:/sbin/nologin
uucp:*:66:1:UNIX-to-UNIX Copy:/var/spool/uucppublic:/usr/libexec/uucp/uucico
www:*:67:67:HTTP server:/var/www:/sbin/nologin
named:*:70:70:BIND Name Service Daemon:/var/named:/sbin/nologin
nobody:*:32767:32767:Unprivileged user:/nonexistent:/sbin/nologin
rgula:*:1000:10::/home/rgula:/bin/csh
dragon:*:1001:10::/home/dragon:/bin/csh
```

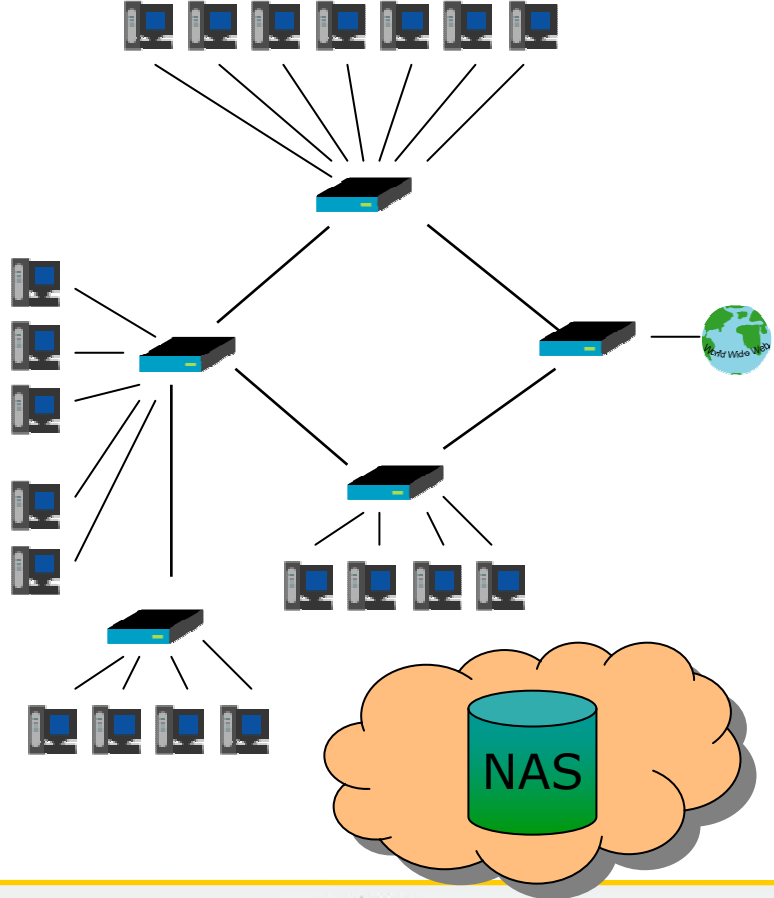
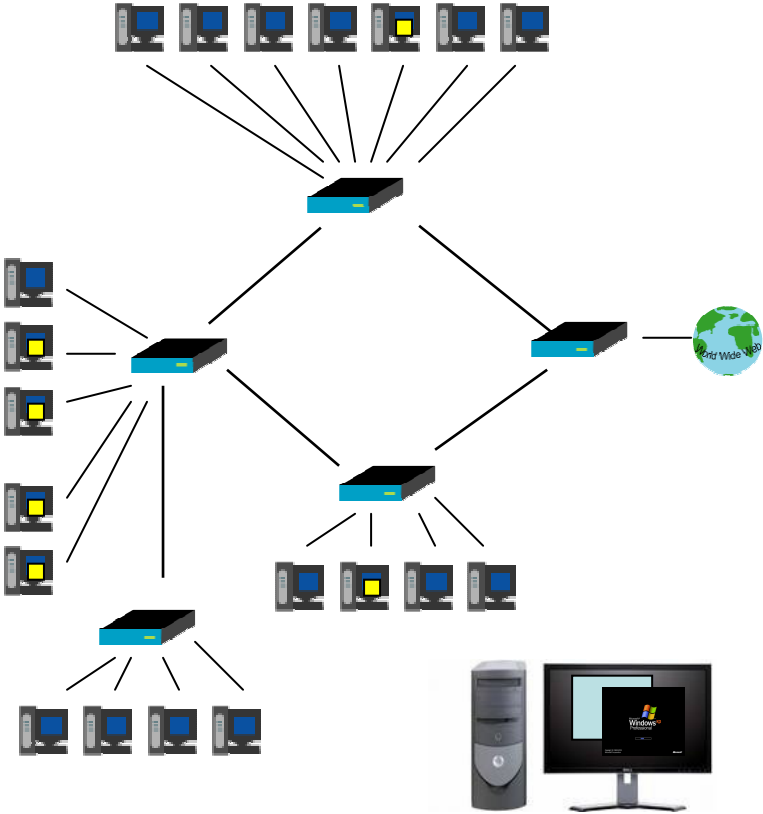
13D4:FF01:A4CA:3A64 ADF0:2423:34AA:0067

```
root:*:0:0:Charlie &/root:/bin/csh
daemon:*:1:1:The devil himself:/root:/sbin/nologin
operator:*:2:5:System &/operator:/sbin/nologin
bin:*:3:7:Binaries Commands and Source,,,:/sbin/nologin
uucp:*:66:1:UNIX-to-UNIX Copy:/var/spool/uucppublic:/usr/libexec/uucp/uucico
www:*:67:67:HTTP server:/var/www:/sbin/nologin
named:*:70:70:BIND Name Service Daemon:/var/named:/sbin/nologin
nobody:*:32767:32767:Unprivileged user:/nonexistent:/sbin/nologin
rgula:*:1000:10::/home/rgula:/bin/csh
dragon:*:1001:10::/home/dragon:/bin/csh
backdoor:*:0:0::/home/dragon:/bin/csh
```

Integrity of File Integrity Checkers



File Integrity Checkers



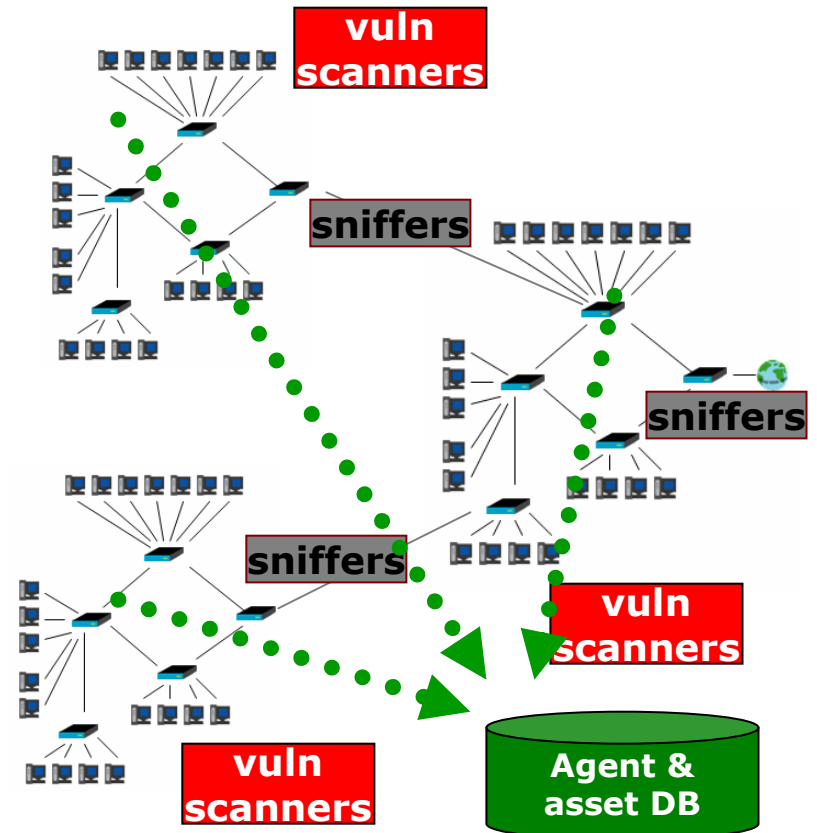
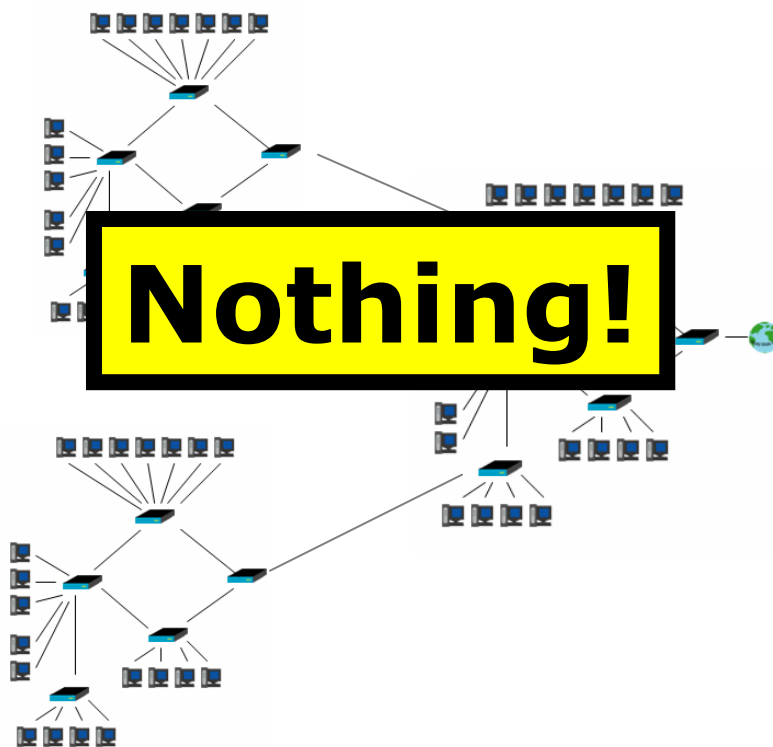
Change Control and Configuration Audits

- Important for forensics!
- Ensures that logging is enabled
 - System logs
 - Microsoft objects
 - User change logging
- If there ever is a data breach, someone will want to know the configuration of the compromised systems
 - PCI or FISMA audits
 - FDCC settings

Asset Discovery

- Also Important for forensics!
- Automatic inventory and asset profiling
 - Agents
 - Scanners
 - Sniffers
 - Network Infrastructure
- If you don't know what is there, you can't plan to collect packets, logs or evidence from it.

Audit and Asset Discovery



Watching the Watchers

- How do you know that your forensics team is not compromised?
- How can you audit your forensic team?
- Where should they report to?
- There should be as much transparency as possible.

Conclusions

- Organizations are deploying a wide array of technology that is useful for performing an analysis of “what happened”
- These technologies can also be more effective at figuring out that “something happened”
- Compliance is the chief driver in these technology advances and requirements

- **rgula AT tenablesecurity.com**
- **<http://www.tenablesecurity.com>**
- **<http://www.nessus.org>**
- **<http://blog.tenablesecurity.com>**

**HIRING PROGRAMMERS
AND SMART SECURITY PEOPLE**