Countermeasures: A Principled Approach

Rita M. Doerr, Ph.D.
Academic Outreach Lead
Cybersecurity Directorate
National Security Agency

Module 3 – Countermeasures and Risk Management

Three Principles

How to reduce risk and mitigate impact:

- Principle 1: **Defense in Depth**
- Principle 2: **Least Privilege**
- Principle 3: **Vigilance**

Module 3 – Countermeasures and Risk Management

Principle 1 – **Defense in Depth**

Every system and network should have multiple layers of defense against intrusion.

Module 3 – Countermeasures and Risk Management

Principle 1 – **Defense in Depth**

Uses multiple security controls throughout a defended network in a layered approach

- **Example:** Multiple firewalls, anti-malware installed on both servers and workstations, and so on
- Also called the "castle defense"

Historical and military precedents:

- Layered defense (multiple lines of defense)
- Delays the enemy's advance and inflicts losses via attrition
- Opposed to a "crust defense"

Module 3 – Countermeasures and Risk Management

Principle 1 – Defense in Depth

Specific Countermeasures

- Firewalls
- Demilitarized Zone (DMZ) or Perimeter Network
- Private Addressing and Network Address Translation (NAT)
- Proxy Servers
- Data Encryption
- Input Validation
- Content Protection
- Anti-Malware Controls
- Configuration Management

Firewalls

A *firewall* monitors and filters network traffic

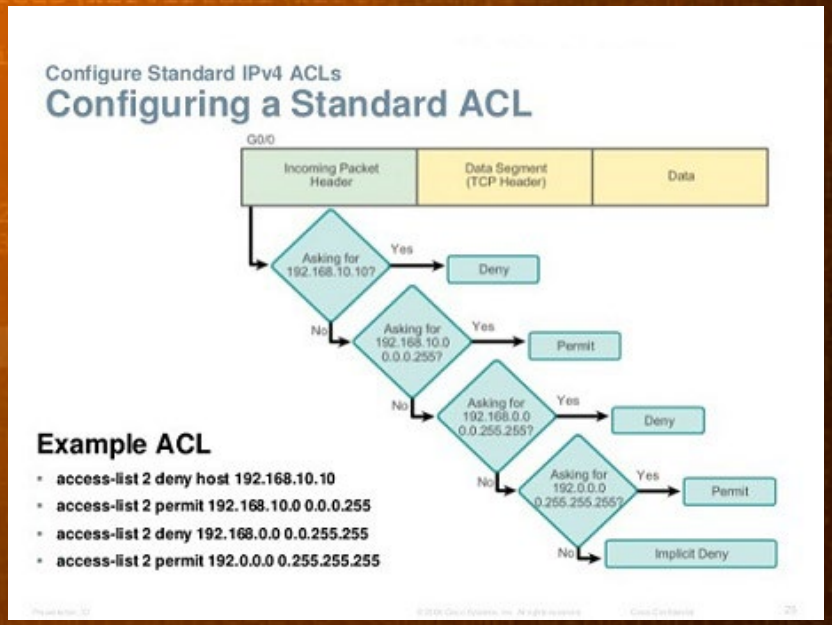
- Applies pre-defined rules
  - First generation: packet filters
  - Second generation: “stateful” packet filters
  - Third generation: application-aware firewalls
- Can filter inbound or outbound traffic
- Can be network-based or host-based

Module 3 – Countermeasures and Risk Management

Firewalls

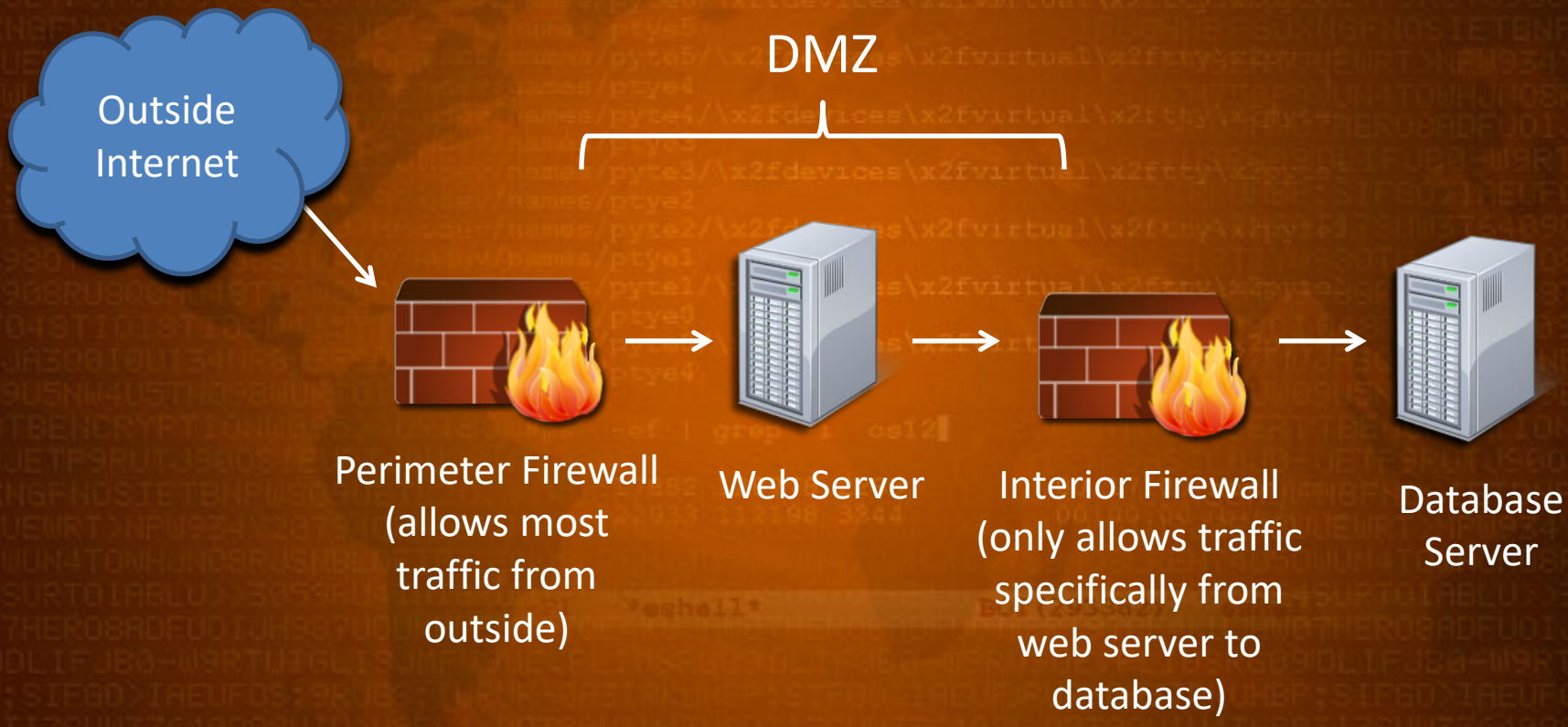
Can be applied in a variety of ways

- Permit communication only from or to trusted entities
- Permit communication only on essential channels or “ports”
- Time out repeated connections from the same source
- Flag or discard suspicious data



Module 3 – Countermeasures and Risk Management

Demilitarized Zone (DMZ) or Perimeter Network



Private Addressing

Private addresses are used inside enclave networks

- Intended to mitigate problem of "running out of IP addresses"
- Packets with private addresses are *dropped* by public routers
- Different enterprises can use the same private addresses

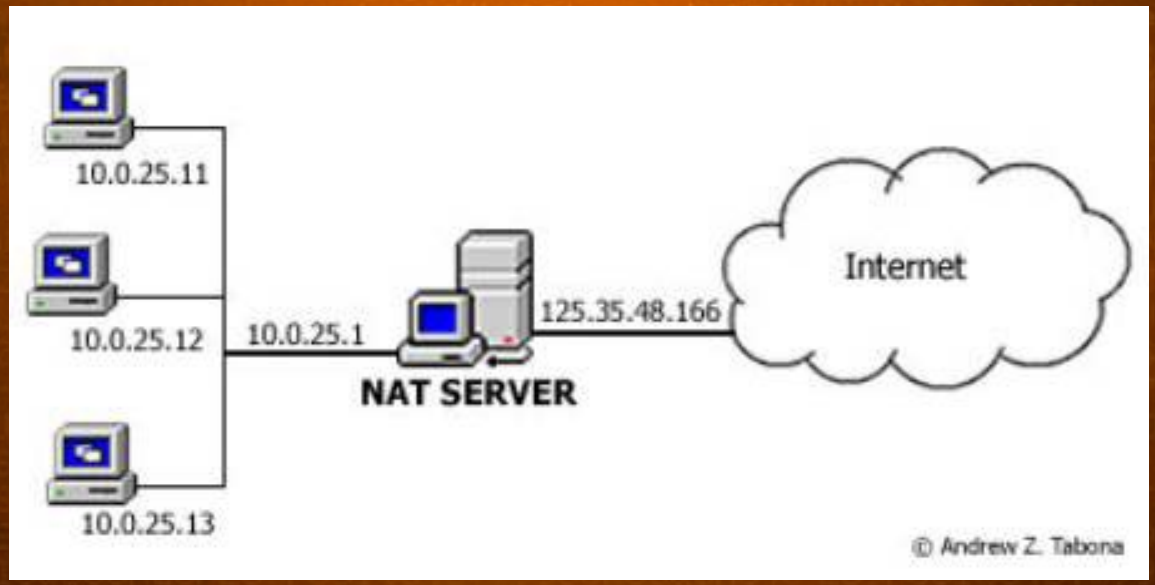
Block Size	First IP Address	Last IP Address	TOTAL
16-bit block	192.168.0.0	192.168.255.255	65,536
20-bit block	172.16.0.0	172.31.255.255	1,048,576
24-bit block	10.0.0.0	10.255.255.255	16,777,216

- **Not very useful by itself . . .**

Network Address Translation (NAT)

Network addresses of packets are modified in transit

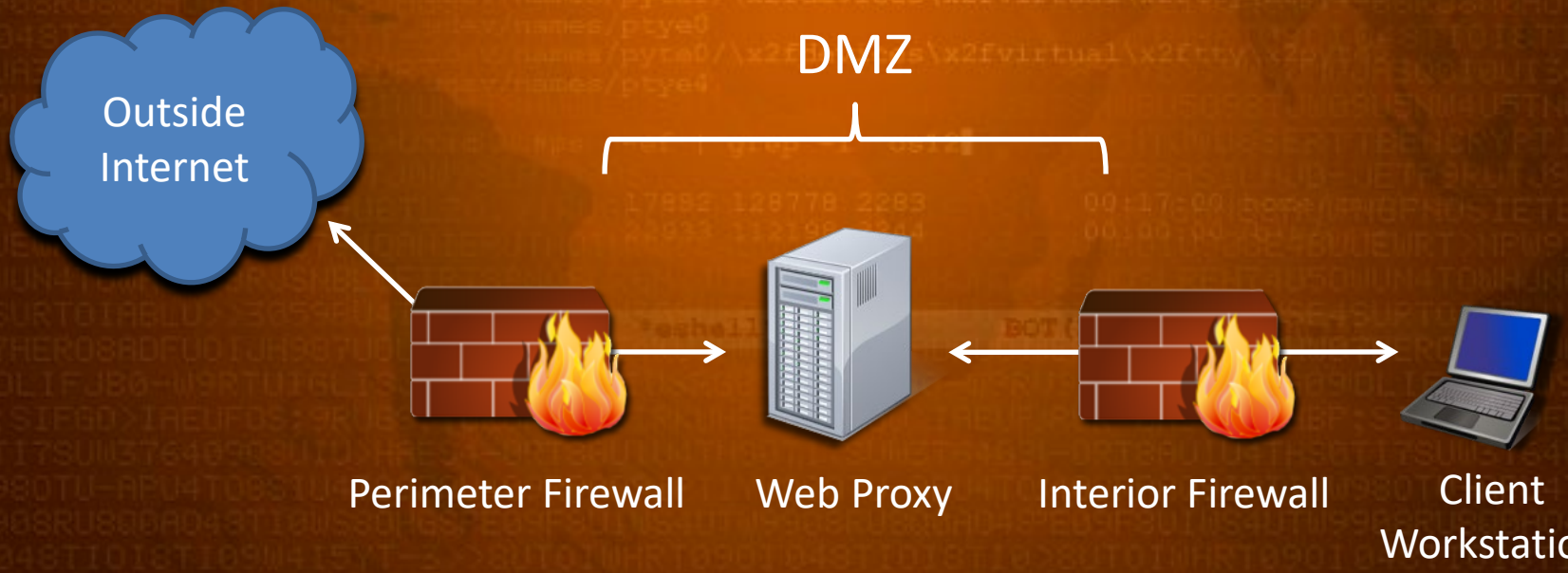
- Entire enclave network can share a single public IP address
- Can be used to obscure the actual addressing scheme of the network



Proxy Servers

Client requests can be routed through a *proxy server*

- Most proxy servers are for web traffic
- Server can simplify and bundle client requests
- Server can also *filter* outbound requests or inbound data



Blacklisting and Whitelisting

Blacklisting: make a list of addresses, sites, applications, or other entities which are *forbidden* to communicate

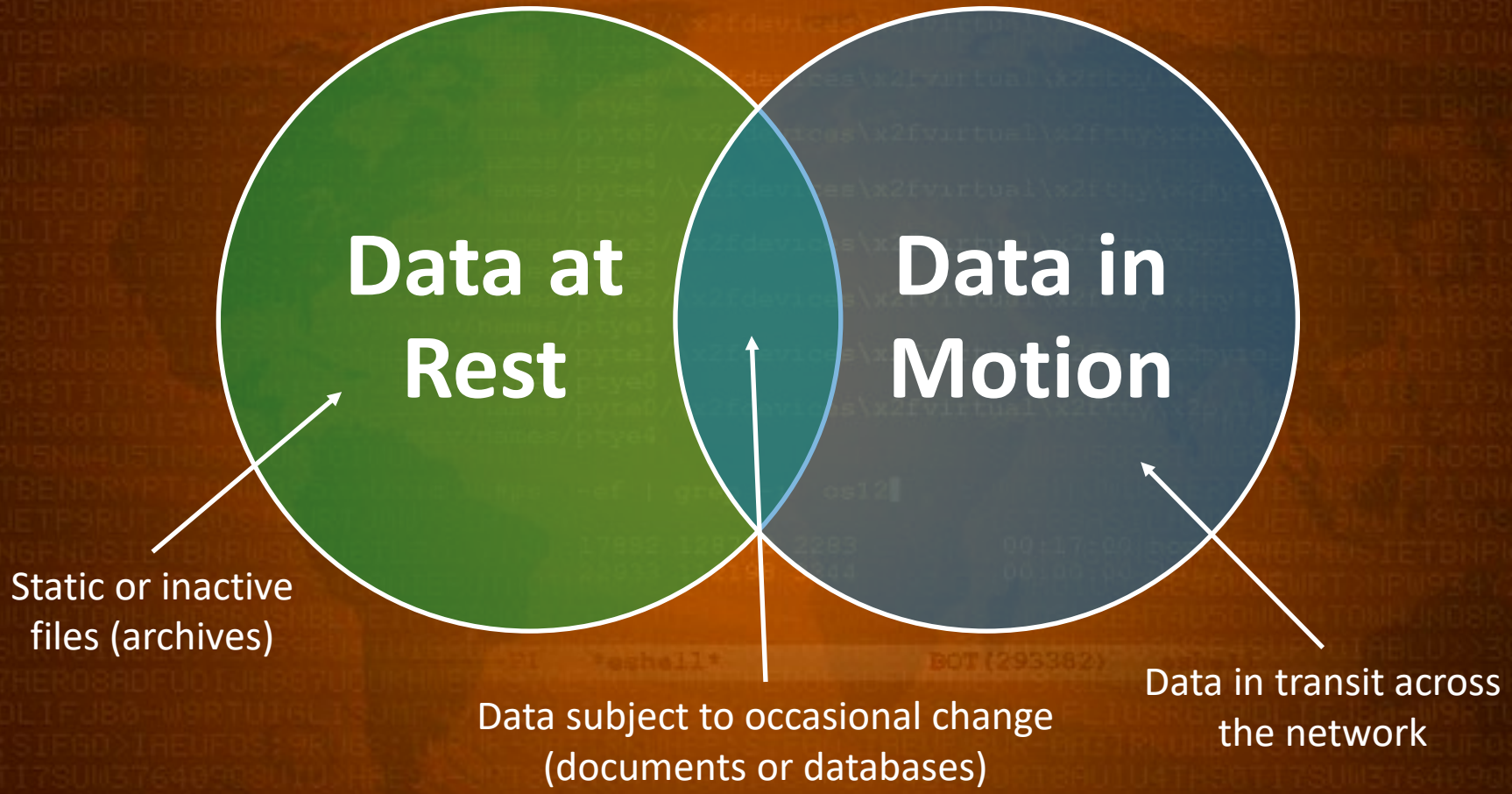
- "Everything not specifically forbidden is allowed"
- Requires that you know sources of malicious data or activity
- Can easily be applied reactively

Whitelisting: make a list of addresses, sites, applications, or other entities which are *permitted* to communicate

- "Everything not specifically allowed is forbidden"
- Requires that you know everything you need for mission

Most effective strategies involve both

Data Encryption



Data Encryption

Data at rest can be either:

- ***Unstructured*** – in files and storage
- ***Structured*** – in databases or applications

In either case, use **strong encryption** (AES, RSA, SHA-256)

Data in motion should be protected using *secure protocols:*

For . . .	Instead of using . . .	Use . . .
Web Access	HTTP	HTTPS
File Transfer	FTP, RCP	FTPS, SFTP, SCP
Remote Shell	telnet	SSH2 terminal
Remote Desktop	VNC	radmin, RDP

Internet Protocol Security (IPSec)

Suite for secure Internet Protocol (IP) communications

- Applies both authentication and strong encryption
- Can work host-to-host or enclave-to-enclave
- Difficult to set up correctly but *very effective*

Input Validation

Check any user-provided data for validity

- Does the data make sense for the field where it was entered?
- Will the data cause an inappropriate action?

Content Protection

Content that doesn't change can be made **unmodifiable**

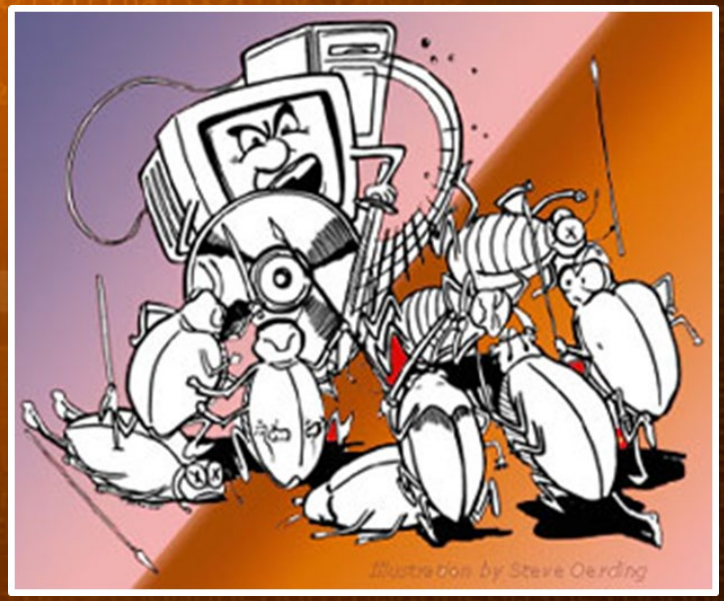
- File system protections . . .
- Or run your website from read-only media!

Encode scripts so an adversary can't easily read them

Anti-Malware Controls

Software examines inbound data for evidence of malware

- "Signatures" or strings of data from known malware
- Connections to suspicious sites
- Unexpected system behavior
- Can operate as a host-based firewall



Patch Management

Patch: an incremental update to software to fix a bug or vulnerability in the code

- Usually distributed for free to legitimate customers
- May be released on a regular schedule ("Patch Tuesday")
- Presents a challenge on large or heterogeneous networks
- Not useful against zero-day exploits

Still one of the most effective countermeasures against hostile network intrusion!

Configuration Management

Make sure systems are configured to be as secure as possible – they aren't necessarily so "out of the box"

Examples:

- Disable automatic execution of macros in documents
- Disable HTML links in emails
- Disable ICMP ("ping") responses
- Disable "promiscuous" mode on network interfaces
- Control the proliferation of trust relationships
- Force periodic re-authentication and session timeouts

Look for the *configuration guide* for your OS or application!

Module 3 – Countermeasures and Risk Management

Configuration Management – Banner Obfuscation

Many servers respond with a *banner* when queried:

```
HTTP/1.1 302 Found
Date: Wed, 04 Dec 2013 16:34:43 GMT
Server: Apache/2.2.16 (Debian)
```

```
220 mail.utopia.org ESMTP Sendmail 8.13.8/8.14.2
```

Intruder can use these to identify vulnerabilities

Banner is usually configurable:

```
HTTP/1.1 302 Found
Date: Wed, 04 Dec 2013 16:34:43 GMT
Server: Generic Web Server
```

Module 3 – Countermeasures and Risk Management

Principle 2 – **Least Privilege**

No account or process on a system should have access to any functions or information it does not need in order to carry out its legitimate function.

Principle 2 – **Least Privilege**

Restricts the *privileges* available to each account or process

Limits the scope of any security control exception

Advantages:

- Makes system or network defense easier to plan
- Limits the damage if the account or process is compromised
- Makes any given intrusion easier to contain

Principle 2 – Least Privilege

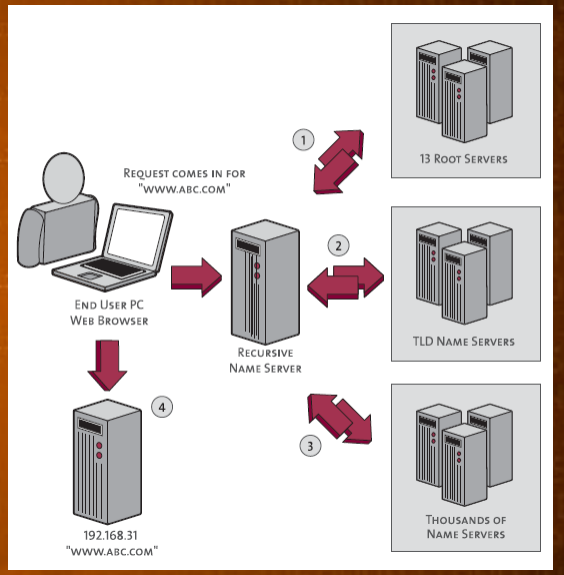
Specific Countermeasures

- Removing Unnecessary Accounts and Services
- Minimizing Processes with Elevated Privileges
- Sandboxing Servers
- Separation of Duties

Removing Unnecessary Accounts and Services

Every service and account represents a potential vulnerability.
Suppose a host is . . .

***DNS Server*: No user accounts!!**



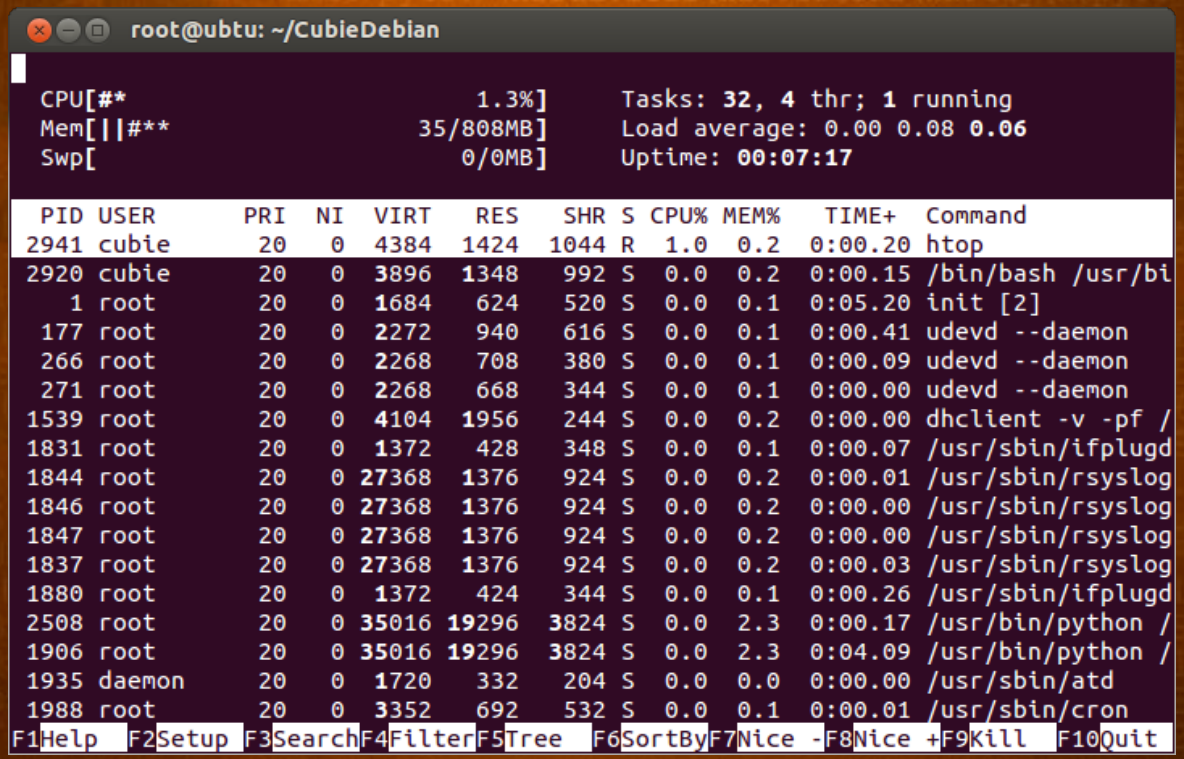
Or . . .

… *a scanning/multimedia host*: No web server on it!!

Module 3 – Countermeasures and Risk Management

Minimizing Processes with Elevated Privileges

Any process that runs as “root” or “Admin” is a potential avenue for *privilege escalation*



Sandboxing Servers

Sandboxing: running an application in a restricted environ
so it has no access or resources other than what it needs to work

- Applications are often run "in a sandbox" during testing
- A server can be sandboxed to limit damage if compromised

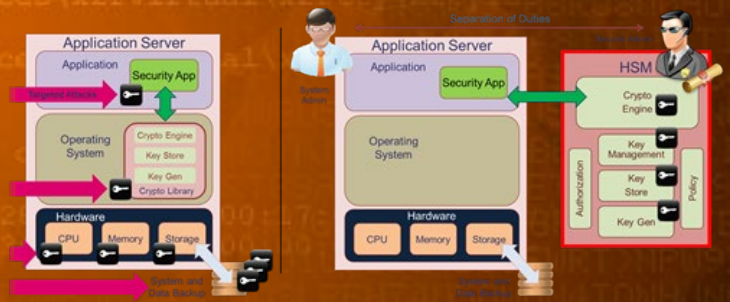
Scenario: Suppose a web server is run under a dummy user account (e.g., *web*). What happens if the server is compromised? What access and privileges might the intruder get?

What if the web server was run under an administrator's account instead?

Separation of Duties

Different functions on a network are handled by different accounts, each with its own least-privilege access

- Helps prevent an adversary from escalating privileges
- Sensitive operations may be divided among privileged users to minimize the impact of a breach



Examples:

- Multiple keys for missile launches
- Database administrator has no general user privileges
- System Administrator role not permitted to perform system audits (ISSO role)

Module 3 – Countermeasures and Risk Management

Principle 3 – **Vigilance**

Every system should be continuously monitored, with an immediate and effective response to any signs of unexpected or unauthorized activity.

Questions?

Thanks for your time! ☺

rita.doerr@cyber.nsa.gov