Threat Risk Analysis

Group Members:
Megan Cutler
JaanusAnja
Boris Plotkin
Daniel Sowinski

Windows Client Systems Threats To

- At risk of obtaining viruses, trojans, or malware.
- Potential disruption of work productivity for users.
- Interruption of access/service to a single host will only affect a single user.

Windows Client Systems

Threats From

- Computer may fall prey to security risks.
  - Pharming, Phishing or other social engineering attacks.
- User installed applications could create vulnerabilities.
- Host could be used to harm internal network.

Windows Client Systems

Risks possible without protection

- An attacked host could reveal account passwords exposing other company resources.
- Host computers could be used as a point from which to launch an attack on other systems.
- A computer could be used as part of a botnet to infect or attack other systems leading to network interruptions.

Windows Client Systems

Proper Protection

- Only permit access to resources that are required by a user.
- Enable restrictions on user accounts.
- Define criteria for passwords.
- Educate users on potential risks and how to avoid them.
- Ensure that all software is up-to-date.
- Configure a local firewall and host based IDS on every client.
- Install and maintain an anti-virus system.

Windows Server Systems Threats To

- Servers provide a centralized collection of tools, applications, and services.
- Susceptible to viruses, malware, and trojans which attack OS vulnerabilities.
- Service disruption for servers providing mission critical services could severely affect the network and users.

Windows Server Systems

Threats From

- Compromised servers may be used to carry out attacks on external targets.
- Servers under the control of an attacker could be used to provide false information.

Windows Server Systems

Risks possible without protection

- Servers are left undefended and open to attack.
- System Administrators will have no knowledge if an attack is taking place.
- Known security vulnerabilities are left open to be exploited.

Windows Server Systems

Proper Protection

- When possible multiple non-dependant services should run on separate servers.
- Limit services offered to only what is necessary.
- Modify and secure accounts.
- Check frequently for information on exploits or vulnerabilities that affect your systems.
- Regularly patch and backup servers.
- Review IDS/Firewall logs.

Linux Server Systems

Threats To

- The organization depends on the services for productivity
- Susceptible to viruses, trojans, worms and hackers of different skill levels
- Interruption of the services can cause significant loss in productivity , reduce the organization's trust and reputation

Linux Server Systems

Threats From

- Vulnerabilities in services and applications (i.e. web) can cause various threats to come from the server.
- Once infected the server may provide malicious responses to requests (DNS cache), spread worms or participate in attacks on other networks

Linux Server Systems

Risks possible without protection

- Vulnerabilities may be attacked or intruded without anyone's knowledge in the organization
- Unprotected networks can become slow and may be prone to Denial of Service attacks
- Increase of threats to the Linux server and its services.

Linux Server Systems

Proper Protection

- Assign permissions with least privilege rule in mind
- Separate components with different risks levels
- Make sure to monitor and maintain security systems after their implementation

Placement of IDSs

- Network IDSs when placed before a firewall can detect attacks on the network as a whole.
- All traffic entering and leaving the network can be inspected by a Network IDS.
- Host based IDSs can detect attacks directed at a individual computer.
- Critical services should have a Host IDS installed.

Placement of Firewalls

- Can actively filter traffic entering or leaving the network.
- Separate the internal network from the external network.
- Will block all unnecessary traffic.
- Multiple firewalls from separate vendors can make attacks more difficult.

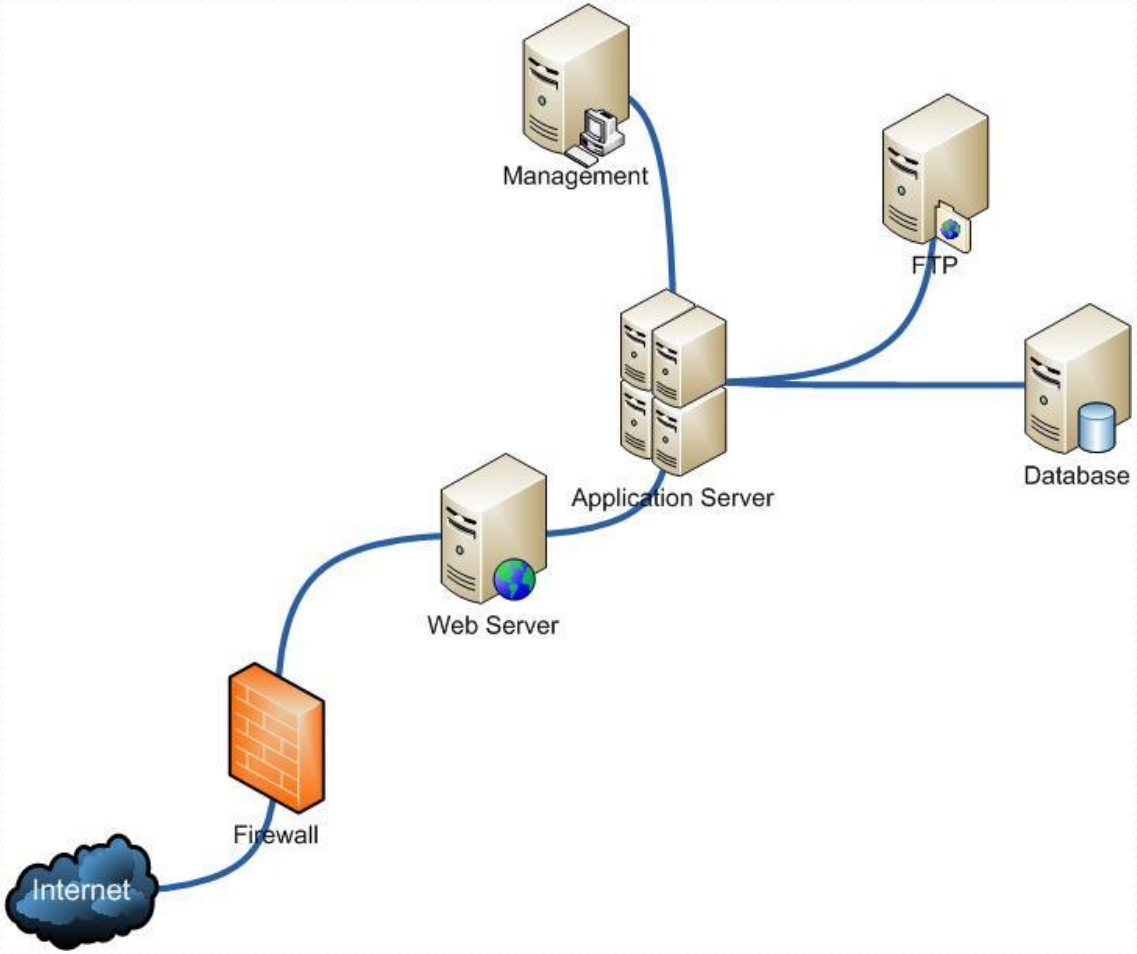
Placement of DMZ

- Provides remote access to services without compromising the internal network.
- A DMZ placed between two firewalls allows for greater control of traffic.
- A HoneyPot placed in a DMZ can help track intrusion patterns.

Utilizing VLANs

- Segregate the network into different areas based on security needs.
- Traffic within VLANs is kept separate from other VLANs.
- Traffic between VLANs can be controlled using access lists.

Insecure Network Design



Secure Network Design