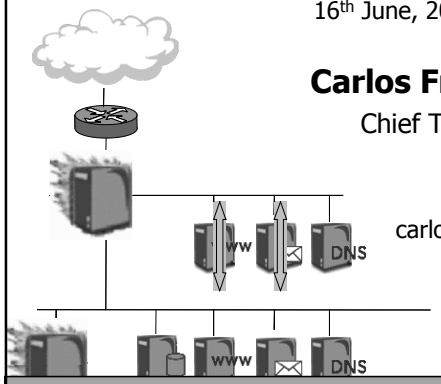
Securing Web Applications...
...at the Network Layer

OWASP Spain Chapter Meeting
16th June, 2006 – Barcelona (ES)

Carlos Fragoso Mariscal
Chief Technical Director

carlos@jessland.net



Goals

- **Consider network security as a defense-in-depth approach for web application security**
- **Learn how security architecture could provide a robust topology to enforce security in web services environments**
- **Have fun with our case-based scenario**

Agenda

- Web Applications
- Security Architecture
- Case Study
- Conclusions
- References

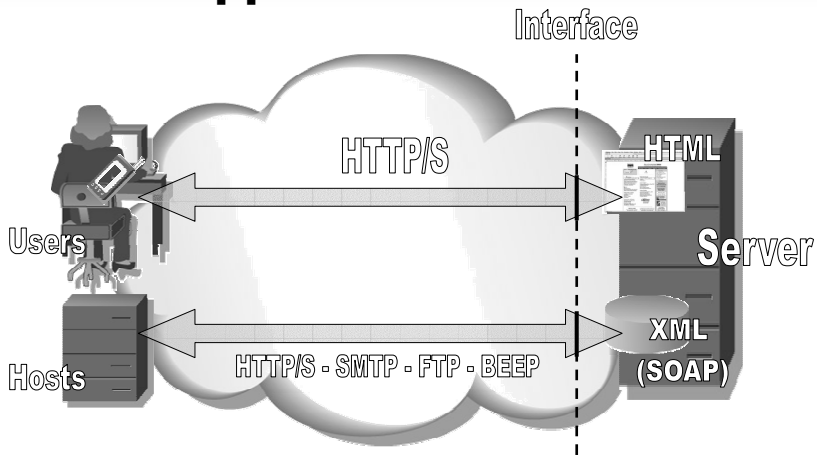
1st OWASP Spain Chapter Meeting

Agenda

- Web Applications
- Security Architecture
- Case Study
- Conclusions
- References

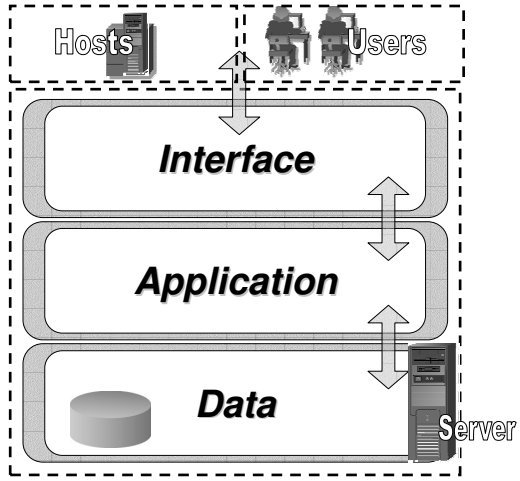
Securing Web Applications at the Network Layer - © 2006 Jessland Security Services www.jessland.net

Web Applications' Interface



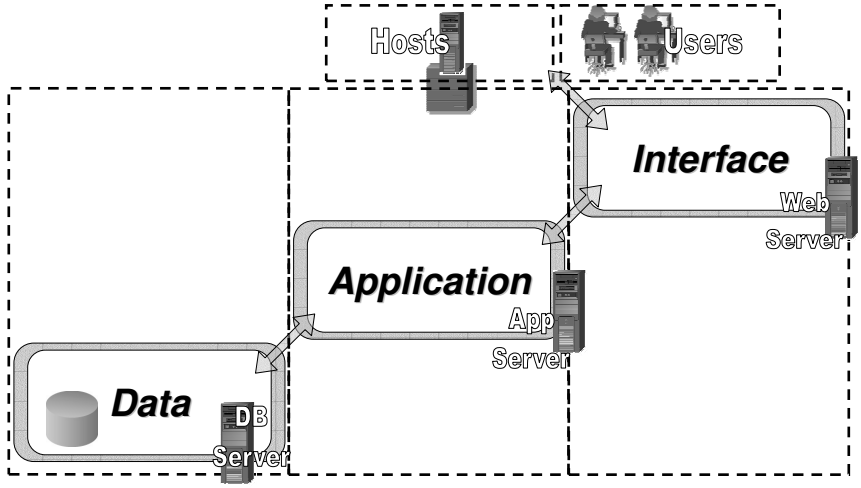
- Web application clients mainly use HTTP protocol as their interface to the application
- Users (B2C) and hosts (B2B) reside on external or business partners networks

Web Application's layered model



- Some web applications are not able to separate interface and application layers so they are just one
- Data layer is commonly a filesystem or a database

Web Application Layers' segmentation



- First operational and security approach is to separate the EVERY layers on DIFFERENT hosts

Agenda

- Web Applications
- Security Architecture
- Case Study
- Conclusions
- References

Design Parameters

- Defense-in-depth
- Technology balance
- Least privilege principle
- Simplicity
- Biodiversity
- Access control
- Operational/Risk balance
- Escalability
- Redundancy

What does Perimeter mean?

Security Areas

- Internet
- Extranets
  - Business partner or remote sites
- DMZ's
  - External
  - Internal
- Intranets
  - Users network
  - Protected network

Devices

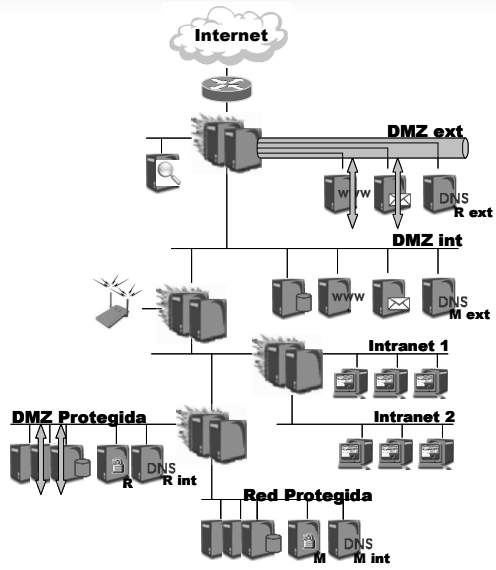
- Firewalls
- Routers
- Switches
- Intrusion Detection/Prevention Systems
- Honeypots and Honeynets
- Security Event Managers
- Servers
- Desktop and mobile end-user systems
- Wireless Access Points
- Hybrids

Network Design step-by-step

- Security policy
- Security levels classification
- Deploy network devices
- Segmentation with firewalls
- Deploy additional security devices
  - IDS/IPS
  - Content inspection
  - VPNs

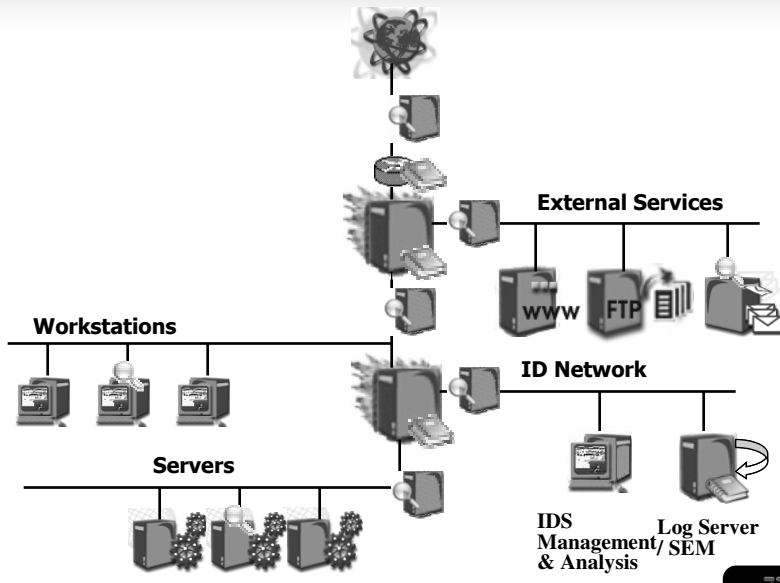
Network Firewalls

- Interconnects different security level networks providing traffic access control
- Technology:
  - Stateless: each packet handled individually
  - Stateful: keeps state of network flows
  - Stateful Inspection: understand application layer protocols
- Value-added features:
  - Load balancing, failover, address translation, VPNs, packet normalization, content inspection, etc.
- Ruleset:
  - Firewall lockdown
  - No logging
  - Log denied
  - Sneaky rule



Network Intrusion/Prevention Systems

- Their job is to provide network audit features and intrusion detection/prevention over the network
- Types: network, node (IDS) and in-line (IDS, IPS)
- Traffic capture: taps, hubs, span ports, balancing...
- Advantages:
  - Easy to deploy
  - Effective
  - Good scalability
- Disadvantages
  - False positives
  - False negatives
  - Non-textual alarms
  - High-volume of data
  - Ciphered traffic
- An IPS is not a firewall !!!



Tips'n'hints ☺

- **Critical information must be placed FAR AWAY from possible risky areas**
- **Network security does NOT patch your hosts for you!**
- **Some critical services have a low rate of possible vulnerabilities because they have been heavily tested**
- **Sometimes information must be replicated to give a limited-scope view**

Prevention 

Detection

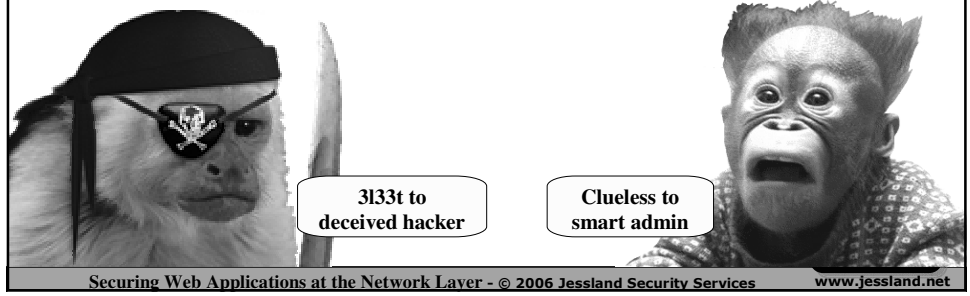
Reaction ! 

Agenda

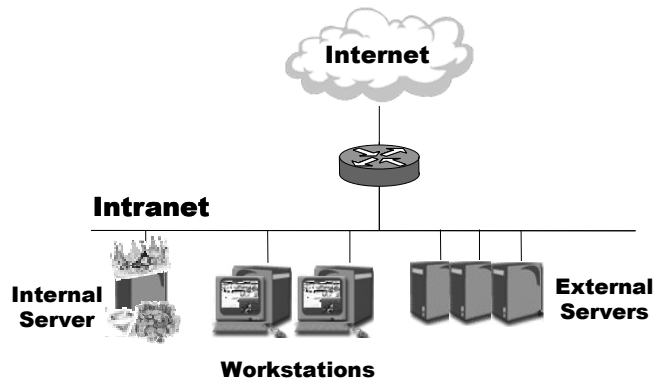
- Web Applications
- Security Architecture
- Case Study
- Conclusions
- References

Security Architecture Case Study

Hackobo vs Armando

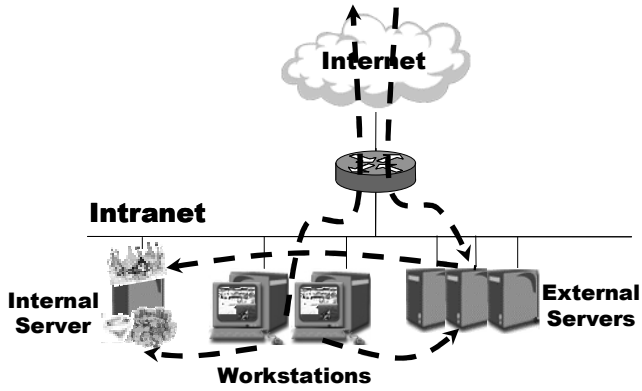


Armando's Network Overview



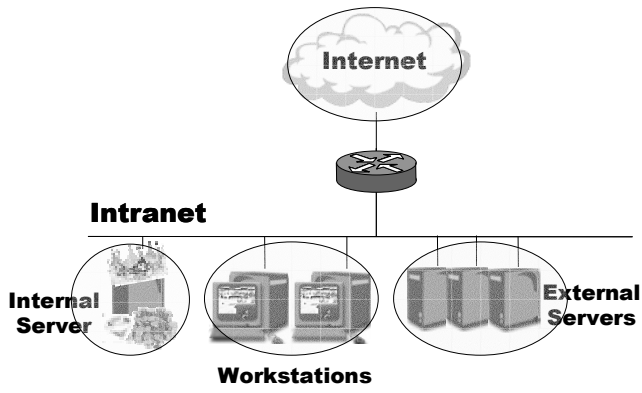
- Corporate network grew **WITHOUT a security-minded approach**
- **Several security INCIDENTS** lead to a security architecture redesign
- Let's help Armando about how to face common issues on his way to a new architecture deployment

Identify how systems talk to each other



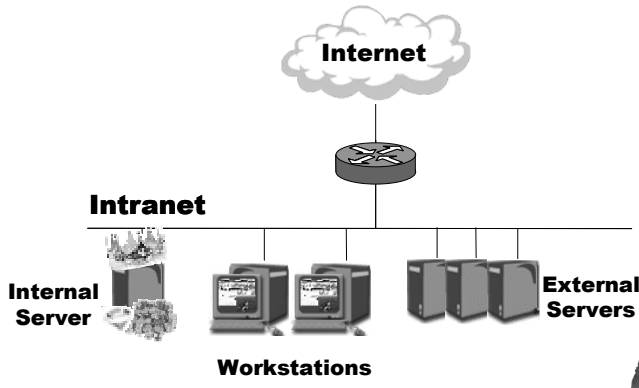
- External users **access external servers**
- Some external servers (web, app, dns, smtp) **need to access internal server**
- Workstation users manage servers and have Internet access

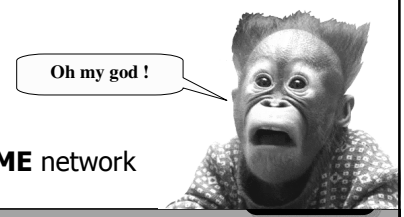
Identifying security areas



- Internal server contains corporate "***JEWELS OF THE CROWN***"
- Workstation users manage corporate infrastructure
- External servers provide services to the outside
- Internet is a public, least-secure, network

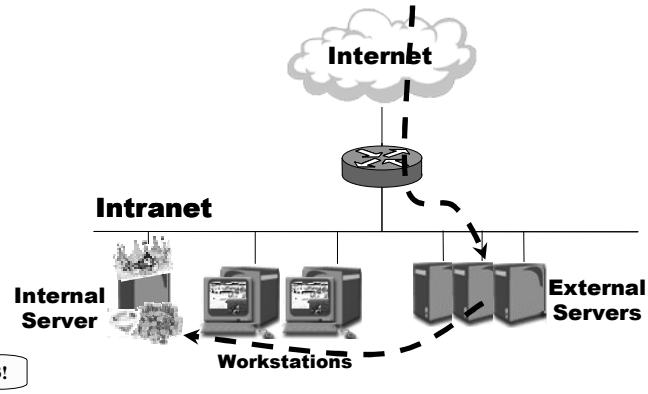
Step 0: Plain Network

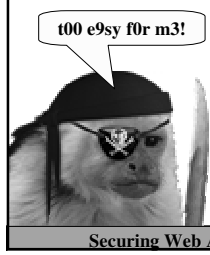




- **LACK of firewalling**
- **DIFFERENT** security areas in the **SAME** network

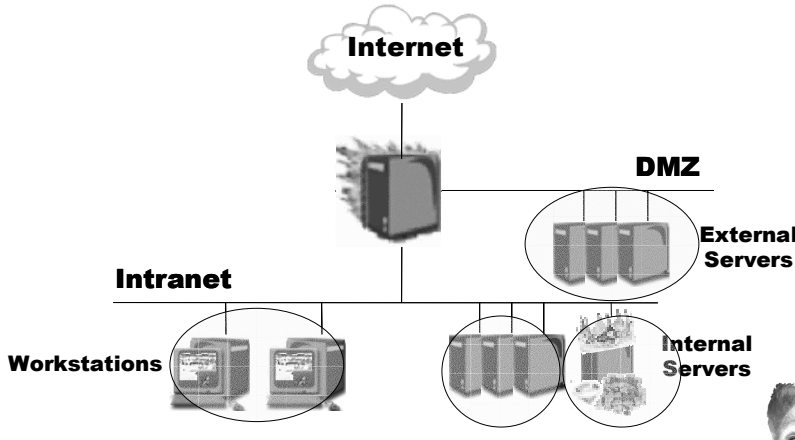
Step 0: Plain Network



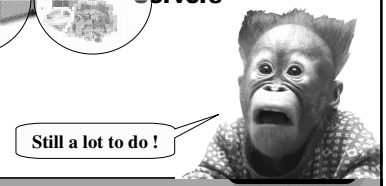


1. **Reconaissance** and **exploit launch** to compromise external web server
2. **Internal reconaissance** attack trying to **compromise** internal workstations or servers

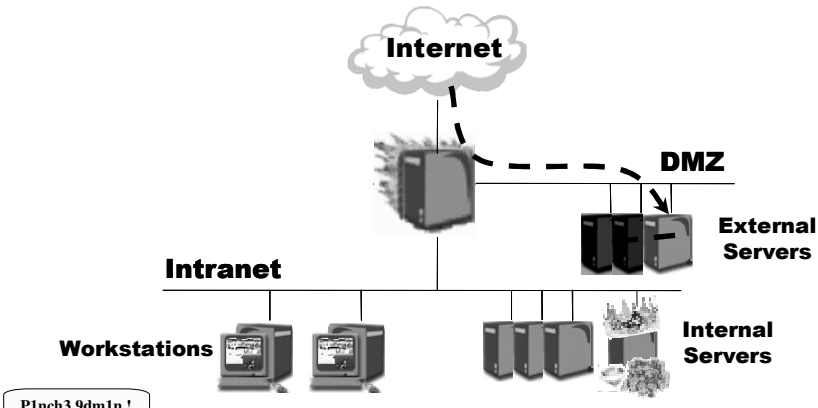
Step 1: DMZ deployment

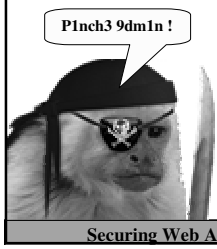


- **Sharing the DMZ** between critical services (dns, smtp) and the web server



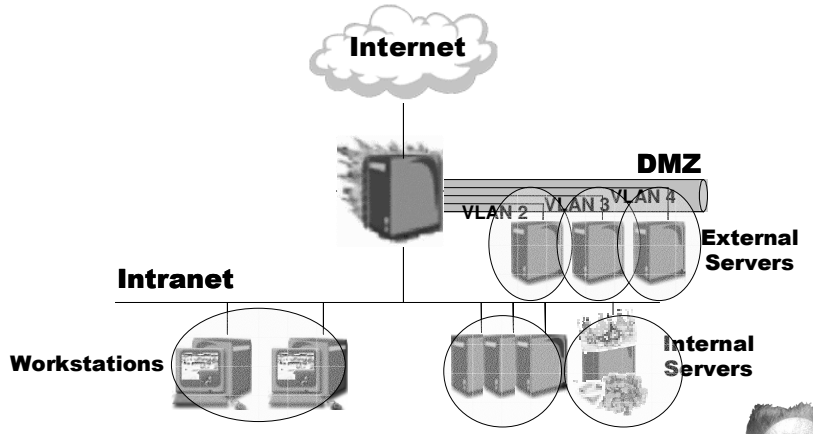
Step 1: DMZ deployment





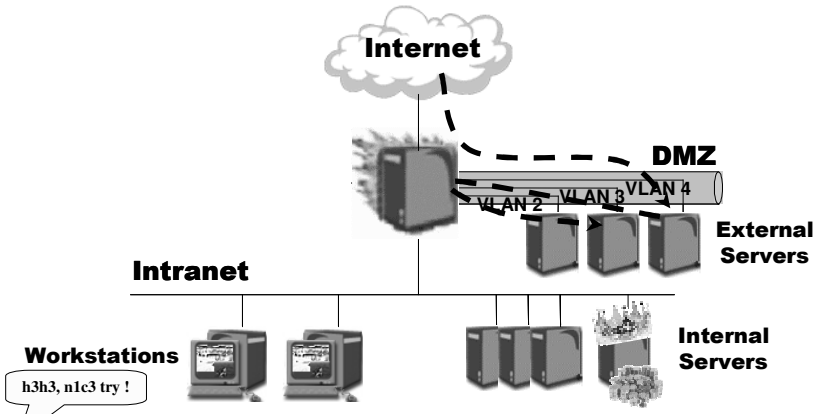
1. Reconaissance and exploit launch to compromise Armando's external web server
2. Firewall allows web server to download hacking tools
3. Local layer-3 compromise or DoS attack against DNS and SMTP external servers

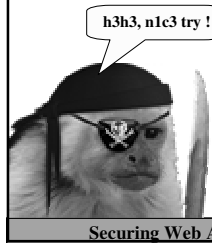
Step 2: VLAN-based DMZ deployment



- Logical isolation (VLAN) on the same physical switch could encourage the hacker to perform L2 DoS or VLAN hopping attacks
- Same software vendor could ease multilayer compromise

Step 2: VLAN-based DMZ deployment

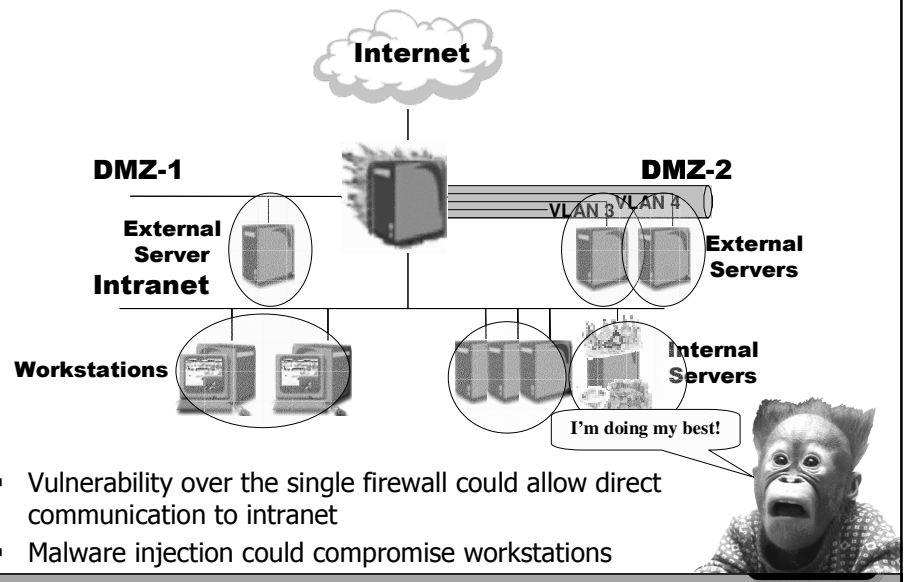




a) Compromise webserver and perform layer-2 vlan hopping in order to try to breach the other servers

b) Launch exploit against smtp or dns server and relaunch it again to get internal access (nicer if possible)

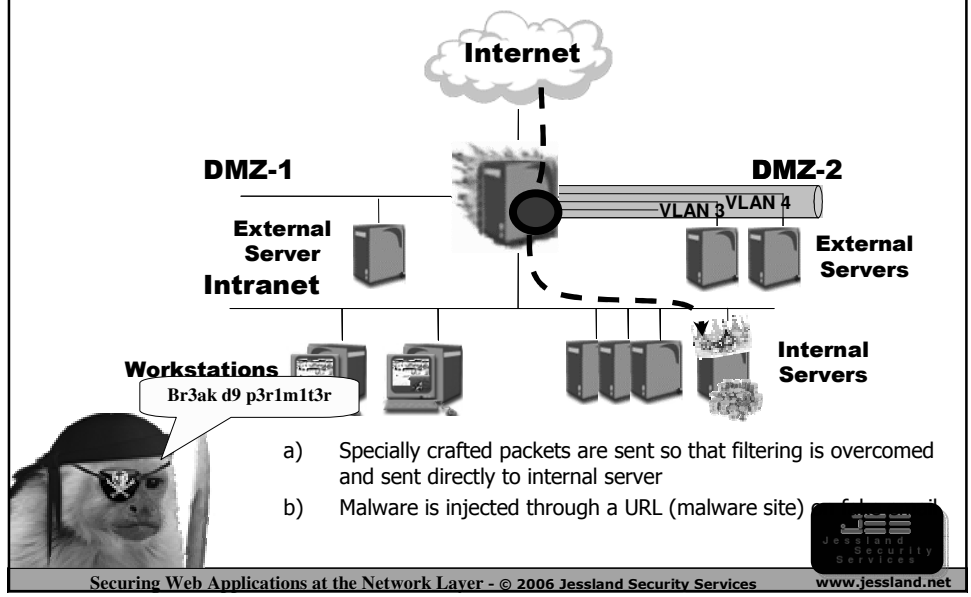
Step 3: Dual public DMZ



- Vulnerability over the single firewall could allow direct communication to intranet
- Malware injection could compromise workstations

1st OWASP Spain Chapter Meeting

Step 3: Dual public DMZ

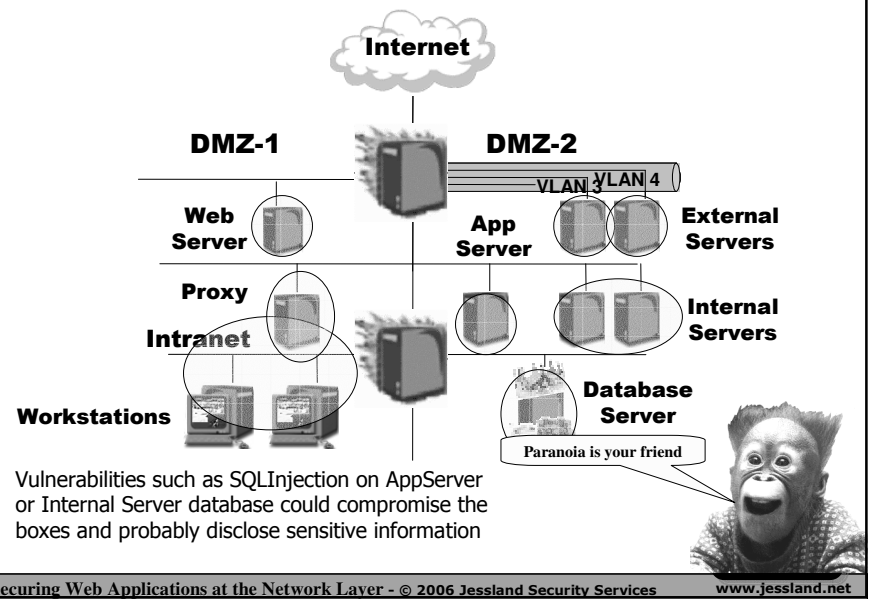


a) Specially crafted packets are sent so that filtering is overcomed and sent directly to internal server

b) Malware is injected through a URL (malware site)

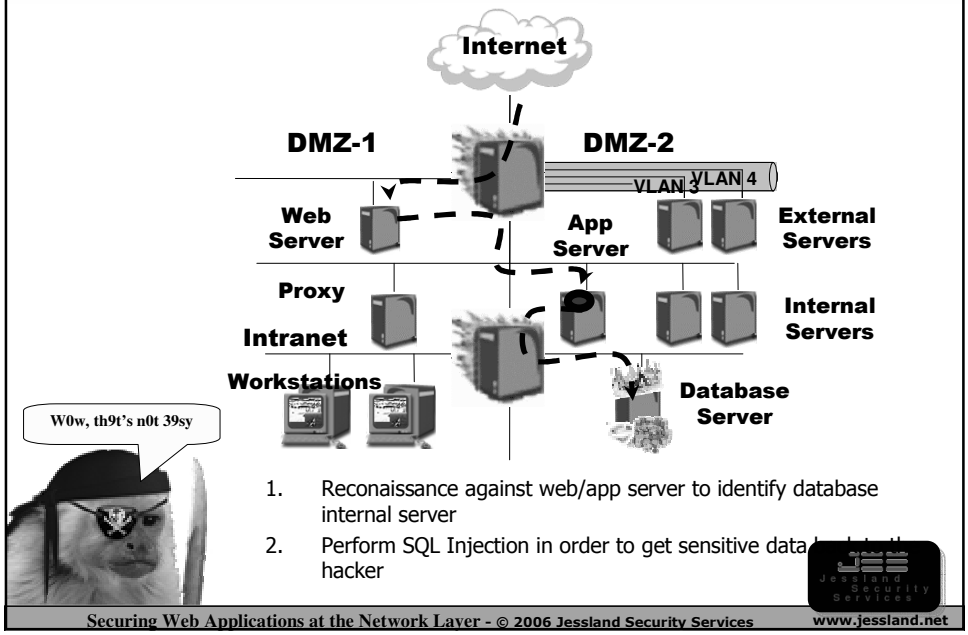
Securing Web Applications at the Network Layer - © 2006 Jessland Security Services www.jessland.net

Step 4: Multilayered service-leg-based double DMZ



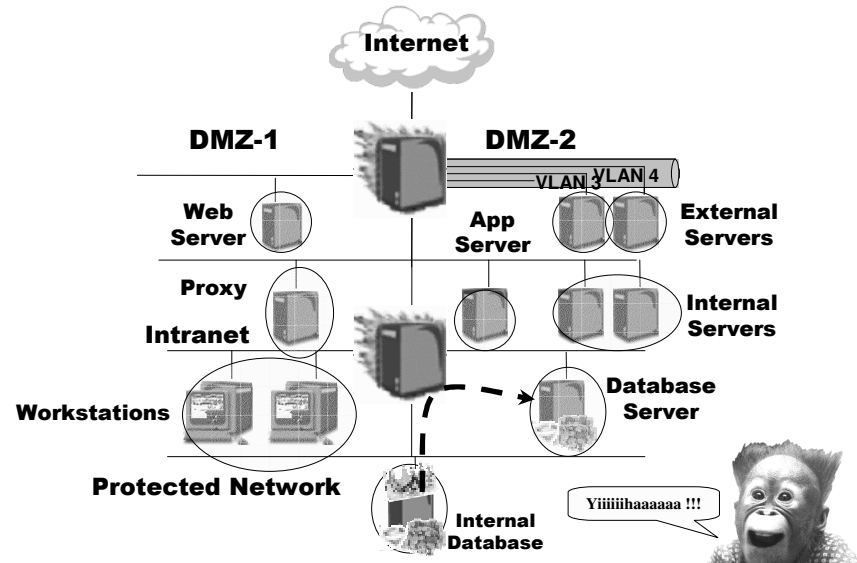
- Vulnerabilities such as SQLInjection on AppServer or Internal Server database could compromise the boxes and probably disclose sensitive information

Step 4: Multilayered service-leg-based double DMZ



1. Reconaissance against web/app server to identify database internal server
2. Perform SQL Injection in order to get sensitive data [illegible] the hacker

Step 5: Protected Network with Data Replication

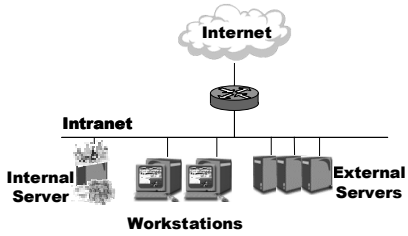


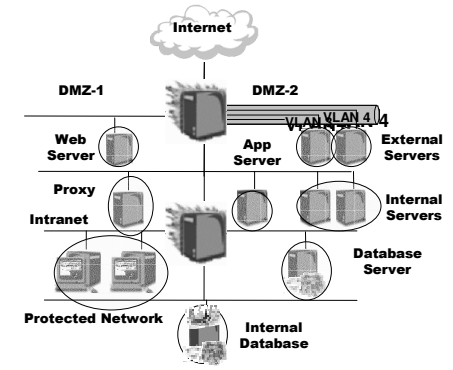
- Database replication of necessary data

Remarkable Security Issues

- Lack of multilayer firewalling
- Sharing of different network security areas
- Outbound traffic control on DMZ areas
- "Relaxed" server patching policy
- Shared resource used for critical information
- Logical vs physical isolation
- OS, Software and hardware biodiversity
- Sensitive data access

Long life to Armando's network





Before

After

Agenda

- Web Applications
- Security Architecture
- Case Study
- Conclusions
- References

Conclusion

- Security architecture definitively helps to improve the global state of security for web services
- It is highly recommended to separate interface, application and data layers
- Knowing your environment is half-the-battle in order to choose a good topology approach
- Place hosts according to their data security level, sometimes splitting or replicating the information is necessary
- What has been described makes thing MORE difficult to the hacker but NOT impossible! ☹

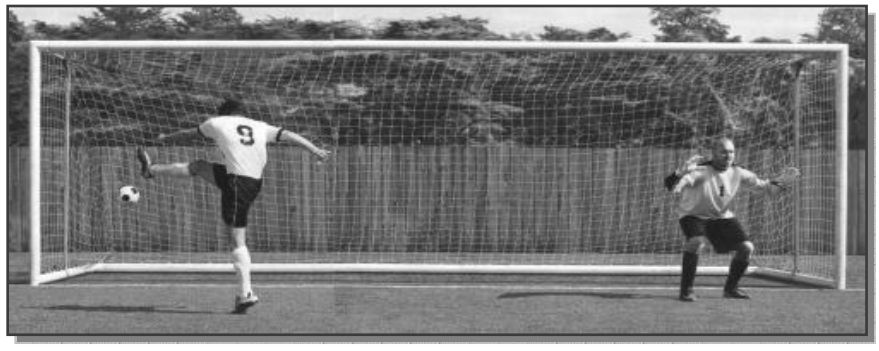
Agenda

- Web Applications
- Security Architecture
- Case Study
- Conclusions
- References

References

- "Inside Network Perimeter Security", S.Northcutt
  ISBN: 0735712328
- "The Tao of Network Security Monitoring", R.Beijlitch
  ISBN: 0321246772
- "Jessland Information Security Knowledgebase (JISK)"
  URL: http://www.jessland.net/JISK.php
- "Protecting your IP network infrastructure", Securite.og
  URL: http://www.securite.org/presentations/secip/
- "Network Intrusion Detection", S.Northcutt & Judy Novak
  ISBN: 0735710082
- "Warriors of the Net"
  URL: http://www.warriorsofthenet.com

Take care of your perimeter !!!

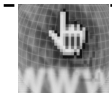


carlos@jessland.net

More information at: http://www.jessland.net

E3B5 8908 57CA 5B67 83DD 9400 085A 29FF D539 69A3

Thank you !!!



http://carlos.fragoso.es carlos@fragoso.es

E3B5 8908 57CA 5B67 83DD 9400 085A 29FF D539 69A3