BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
(nishit.narang@pilani.bits-pilani.ac.in)

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 4: Enterprise Security – Securing the Network & Systems

Enterprise = Network + Systems + Data + Humans + …

Source Disclaimer: Content for many of the slides is from the course Textbook(s). Refer Course Handout for list of Textbooks.

Enterprise Security

Securing the Network (Contd.)

IDS/IPS

- Intrusion detection and prevention technology has remained a mainstay at the network perimeter
  - While several firewall technologies are integrating intrusion prevention into their offerings, there has not been a complete shift to this implementation
- Intrusion detection is a method for detecting an attack but taking no action
  - this has been abandoned at the network perimeter when a breach is undesirable
  - it seems to still have a significant implementation in the internal network server segments to passively observe the behaviors of internal network users
  - has all the detection logic of intrusion prevention but without the ability to actively mitigate a threat
- Intrusion prevention is similar to intrusion detection, but has the capability to disrupt and mitigate malicious traffic by blocking and other methods
  - Many IPS devices have purposefully built denial of service mitigation technology
  - can be deployed at the network perimeter
  - should also be considered for implementation in the internal network to protect the most critical assets within the organization
- As the attacks have become advanced, there is debate on the overall advantage of the IDS/IPS
  - However, a defense in-depth strategy is best implemented by including IDS/IPS as an essential network protection mechanism

IDS/IPS: Detection Methods

- IDS/IPS devices use a combination of three methods to detect and mitigate attacks
  - behavior, anomaly, and signature
  - initial IDS/IPS systems were specialized in one method or another
  - Today, it is rare to find a detection method without the others
  - Also because attacks are not always as simple as protocol misuse or a known Trojan signature

IDS/IPS: Behavior Analysis

- Behavioral analysis takes some intelligence from the platform to first gain an understanding of how the network "normally" operates
  - what systems communicate with other systems, how they communicate, and how much
- Any deviation from this baseline becomes an outlier and triggers the IDS/IPS based on this behavioral deviation
  - Example, if a system is compromised, the connection rates exceed what is common for the system
- The primary caveat with this approach is the mistake of baselining malicious traffic within standard network traffic as "normal“
  - This common and almost unavoidable mistake requires the other detection methods to bring real value

IDS/IPS: Anomaly Detection

- Malware writers often attempt to masquerade their application as a legitimate application
  - this method is commonly employed by chat clients, bit torrent, and other P2P applications
  - Such apps are typically not permitted, so developers have written the applications to look harmless
- Anomaly detection at the network perimeter can be extremely effective in analyzing inbound HTTP requests where the protocol is correct, but there has been some manipulation to the packet
- Nonetheless, understanding the RFC specifications for every protocol is a daunting task!!

IDS/IPS: Signature-based Detection

- A consistent method to detect known malicious attacks
- IDS/IPS looks for known patterns in the packets being inspected
- When a signature or pattern match is found, a predetermined action is taken
- Detects the most common, generic attacks
- Ineffective for the more sophisticated attacks
- Another annoyance with this method is the high rate of false positives

With a majority of attacks targeted at the network being Distributed Denial of Service (DDoS) and SQL injection (SQLi), signature-based IPS can be very effective in mitigating these attacks and continue to provide value at the network perimeter

APT Detection and Mitigation

- APT = **Advanced Persistent Threat**
- Are complicated and well disguised malware
  - use complicated zero-day vulnerabilities, multi-encoded malicious payloads, encryption, obfuscation, and clever masquerading techniques
- APT mitigation solutions work by providing a safe environment
  - usually virtualized instances or sandboxes of operating systems are employed, where malicious software can run and infect the operating system
  - The tool then analyzes everything the malicious software did, and decodes the payload to identify the threat and create a "signature" to mitigate further exploitation
  - Technology in this space is new and relatively less known
- Some tools are appliance-based. The decoding and analysis happens on the box. Other vendors provide the service in the cloud

Several manufacturers in the IDS/IPS and NGFW technology areas have made significant progress in providing APT detection and mitigation, both on the box and in the cloud

Securing Network Services (NS)

- Enterprises provide and leverage Internet services such as DNS, e-mail, and file transfer
  - The latest malware threats utilize these common services in order to redirect internal hosts to Internet destinations under the control of the malware writers
  - However, with correctly implemented architecture, this scenario would mostly be a mute point, and with additional security mechanisms, a rare occurrence
- In the next few slides, we will discuss the security implementations for DNS, Email, File Transfers and Websites

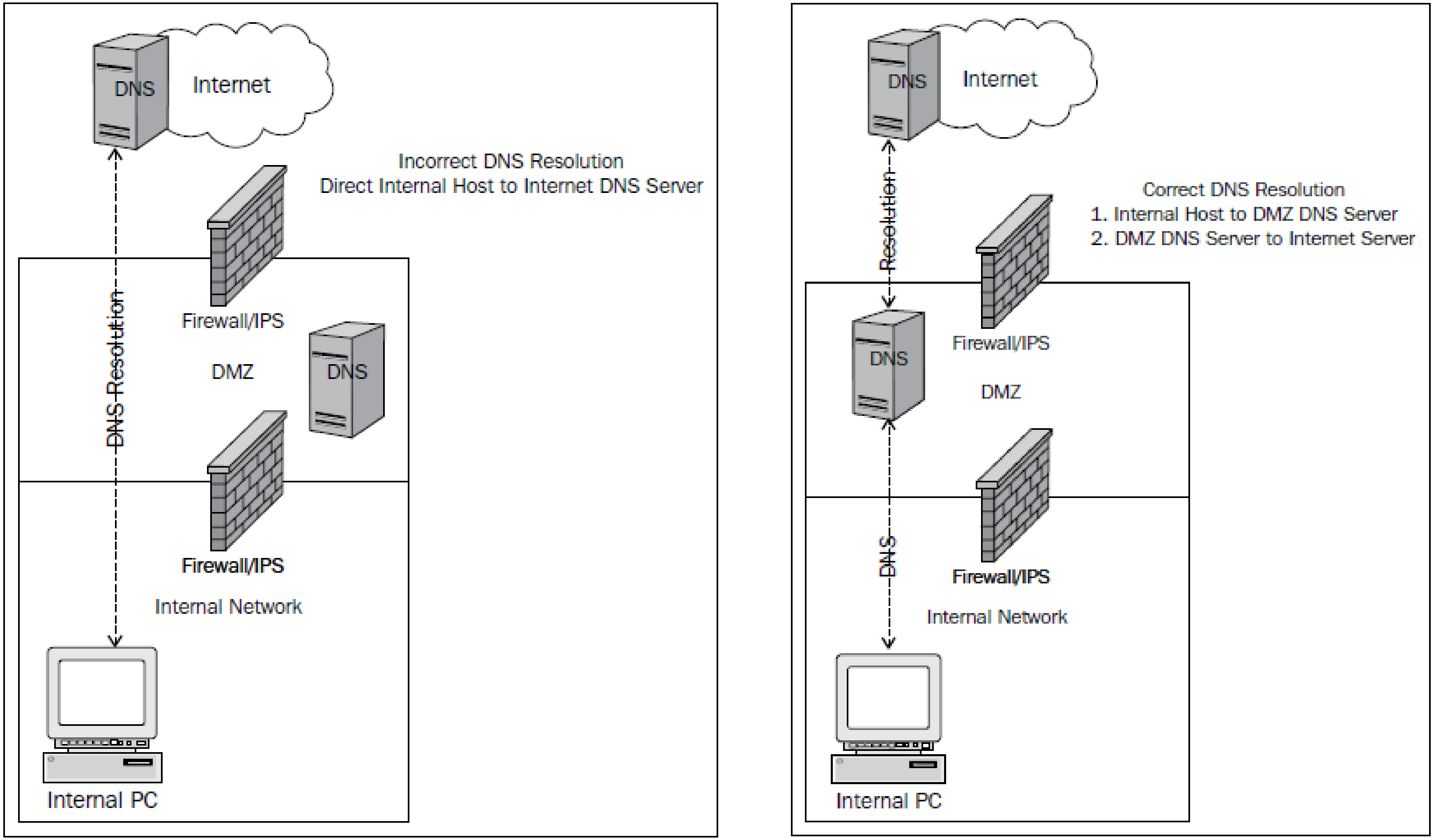
NS: DNS Service Security

- DNS provides a mapping of an IP address to a fully qualified domain name
- A system can be directed anywhere on the Internet with DNS, so the authenticity of the source of this information is critical
- This is where **DNS Security Extensions** (**DNSSEC**) come into play
  - provide authenticity for DNS resolver data
  - DNS data cannot be forged and attacks like DNS poisoning, where erroneous DNS is injected into DNS and propagated, resulting in pointing hosts to the wrong system on the Internet is mitigated. This is a common method used by malware writers and in phishing attacks
- Another area of security in regards to DNS implementation are DNS zone transfers
  - mechanism used in DNS to provide other DNS servers with what domains the DNS server is responsible for and all the details available for each record in the zone

NS: DNS Resolution

- DNS resolution can make for easy exploitation if there is no control on where the mapping information is obtained
  - This has been the main method used by the Zeus botnet
  - Hosts are pointed to maliciously controlled Internet servers by manipulating DNS information
  - The method also relies on compromised or specifically built DNS servers on the Internet, allowing malware writers to make up their own, unique and sometimes inconspicuous domain names

NS: DNS Resolution (2)



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

NS: DNS Zone Transfer

- A DNS zone transfer should be limited to only trusted partners and limited to only zones that need to be transferred
  - An enterprise may have several domain names for various services they provide to business partners and employees that are not "known" by the general public
    - Example, office-specific records, a VPN URL, SIP address for VoIP, etc
  - While the fact remains that if the service is available on the Internet, it can be found, a simple zone transfer reduces the discovery process significantly
- There may be internal and external DNS implementations with records specific to the network areas they service
  - the internal DNS server may have records for all internal hosts and services, while a DNS server in the DMZ may only have records for DMZ services
  - it is critical to keep the records uncontaminated from other zones
  - Specifically, TXT may give too much information that can be used in a malicious manner against the enterprise

NS: DNSSEC

- Most prevalent DNS attack is **DNS poisoning**, where the DNS information on the Internet is poisoned with false information, allowing attackers to direct clients to whatever IP address they desire
- Security extensions have been added to the DNS protocol by the **Internet Engineering Task Force (IETF) DNS Security (DNSSEC)** specification
  - provides security for specific information components of the DNS protocol in an effort to provide authenticity to the DNS information
- The importance of DNSSEC is that it is intended to give the recipient DNS server confidence in the source of the DNS records or resolver data that it receives

NS: Email Service Security

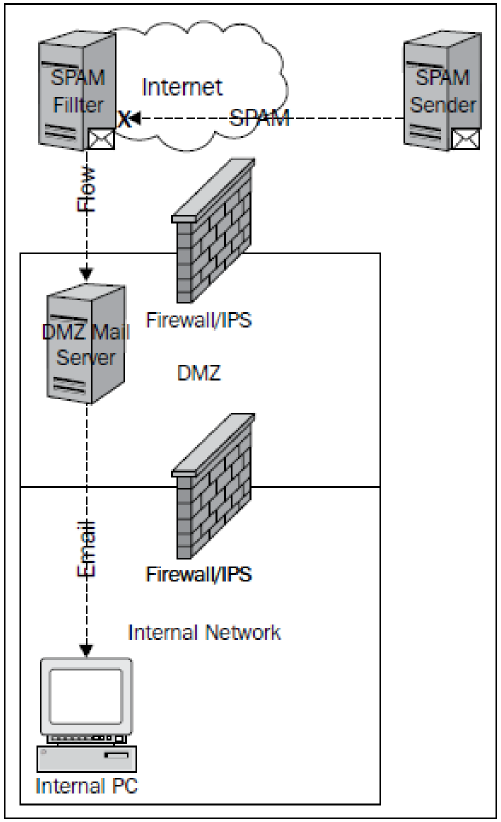
- Email service is a critical business function
- With the increased growth and acceptance of cloud-based services, e-mail is amongst the first to be leveraged
- Some enterprises have already moved their e-mail implementation to the cloud
  - + Enables lower cost and *as-a-service* implementation
  - - enterprises have lower control over email security
- The next few slides will cover common e-mail threats and present methods to secure e-mail services

NS: Spam Filtering

- E-mail is one of the most popular methods to spread malware or lead users to malware hosted on the Internet
  - Most often, this is the single intent of unwanted e-mails in the form of SPAM
  - Receiving SPAM and becoming the source of SPAM while being used as a relay are two sides to the same coin
- Methods to protect the enterprise from SPAM include cloud-based and local SPAM filtering at the network layer and host-based solutions at the client
  - A combination of these methods can prove to be most effective

NS: Spam Filtering @ Cloud

- Works by configuring the DNS **mail record (MX)*** to identify the service provider's e-mail servers
  - This configuration forces all e-mails destined to e-mail addresses owned by the enterprise through the SPAM solution filtering systems before forwarding to the final enterprise servers and user mailbox
  - Outbound mail from the enterprise would take the normal path to the destination as configured, to use DNS to find the destination domain email server IP address



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

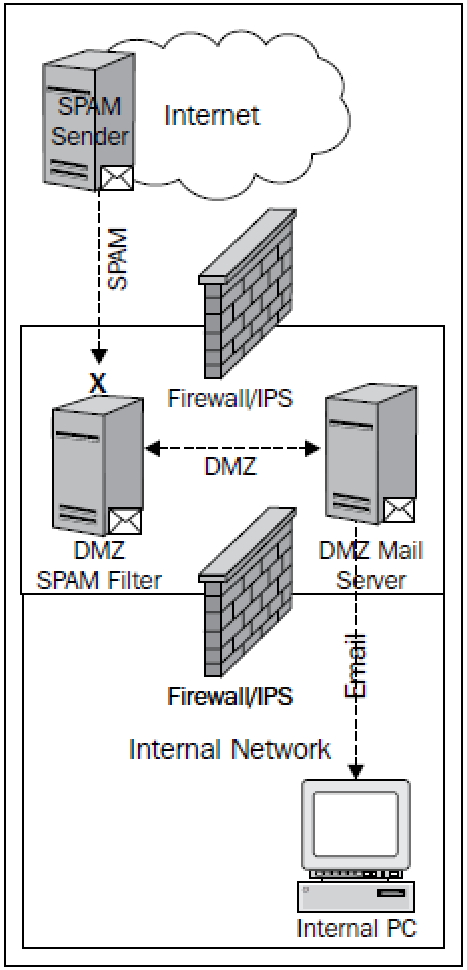
A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name. It is a resource record in the Domain Name System (DNS). It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing and redundancy. Source: Wikipedia

NS: Spam Filtering @ Cloud (2)

- Pros and Cons:
  - + Zero or limited administration of the solution
  - + Reduction in Spam traffic
  - + Reduction in malware and other threats
  - - Significant cost, depending on service fee structure
  - - lack of visibility and control of filters
  - - service failure => no email or unwanted delays
- Enterprise needs to do cost-benefit analysis before taking this option
  - Cost of service
  - Implicit cost (e.g. due to loss of service, or unwanted delays)
  - Benefits (savings due to reduction in spam emails or malware threats)

NS: Local Spam Filtering

- Only an option when the enterprise is not using a web-hosted/cloud-based email solution
  - With web-based e-mail hosting, the SSL connection exists from the user's browser or e-mail client to the hosted e-mail servers
  - SSL decryption could be possible, but the overhead and privacy implications should be weighed carefully
    - Decrypting SSL by presenting a false certificate in order to snoop breaks SSL theory and is considered a *man-in-the-middle* attack
- Several solutions exist to provide SPAM filtering and e-mail encryption in one appliance
  - may play a role in the enterprise data loss prevention and secure file transfer strategies, providing more than just SPAM filtering



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

NS: Local Spam Filtering (2)

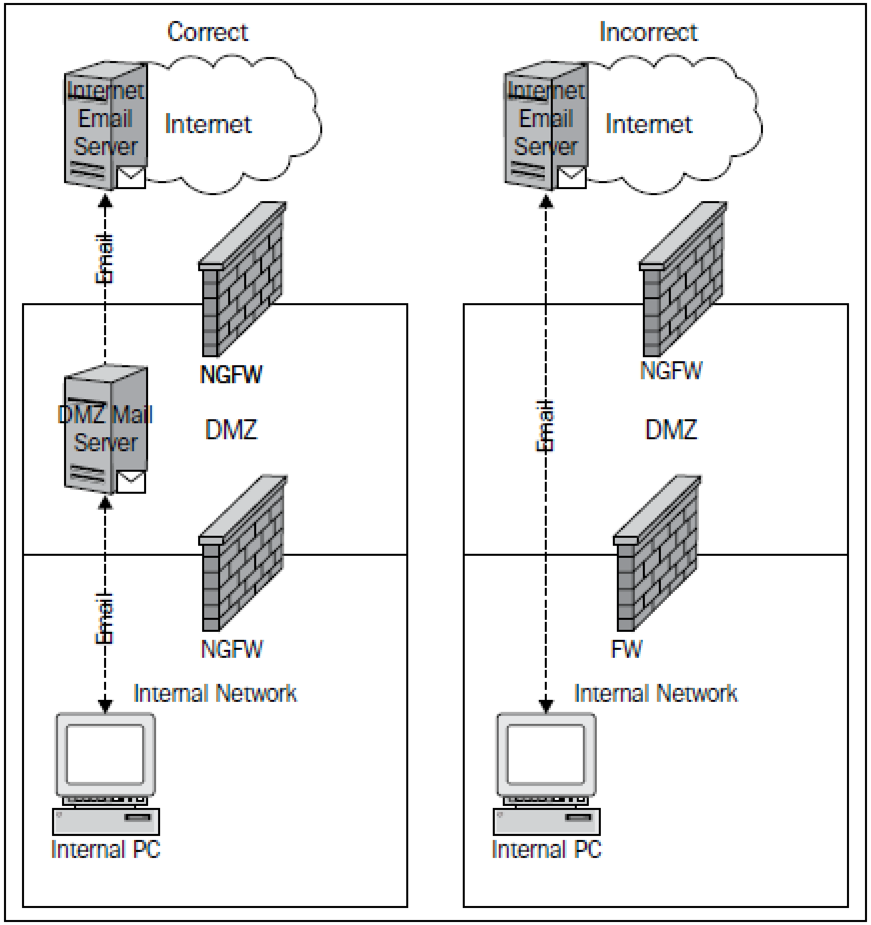
- Pros and Cons:
  - + more control over configuration of filters
  - + vendor continuously updates the appliance to include new block list updates and signatures
  - + ability to also own the DNS infrastructure that tells other e-mail systems where to send e-mail
    - In the event of appliance failure, e-mails can be routed around the failure using DNS to maintain the e-mail service
  - - Technically, a debatable solution if web-based email solution is used
- Again, an enterprise must make an assessment for operational feasibility prior to making the decision to locally detect and mitigate SPAM

NS: Spam Relaying

- Misconfiguration of the enterprise mail servers may lead to exploitation in the form of using the servers as a SPAM relay
  - method uses the server's lack of sender authentication and capability to send e-mails from domains which it does not have authority to send e-mail
- Unfortunately, this misconfiguration is common
  - Internet facing e-mail systems only authenticate for the internal mail relay
  - Internal servers for the requirement of non-human processes to send e-mails, such as the alerting mechanism on a security system
    - The internal server should still have restrictions on sending domains, to avoid the system being misused to send other spoofed e-mails

NS: Spam Relaying (2)

- Prevention:
  - Implement e-mail controls at the firewall to ensure that only the internal mail servers are able to directly send e-mails to the Internet
  - This method reduces the potential impact of end system malware, designed to send SPAM from inside the network
  - Some malware is specifically designed to blast e-mail SPAM from the infected system, thus getting the enterprise blocked by services such as SPAMHAUS



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise