ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Network and Operational Security Practices

COM-402: Information Security and Privacy

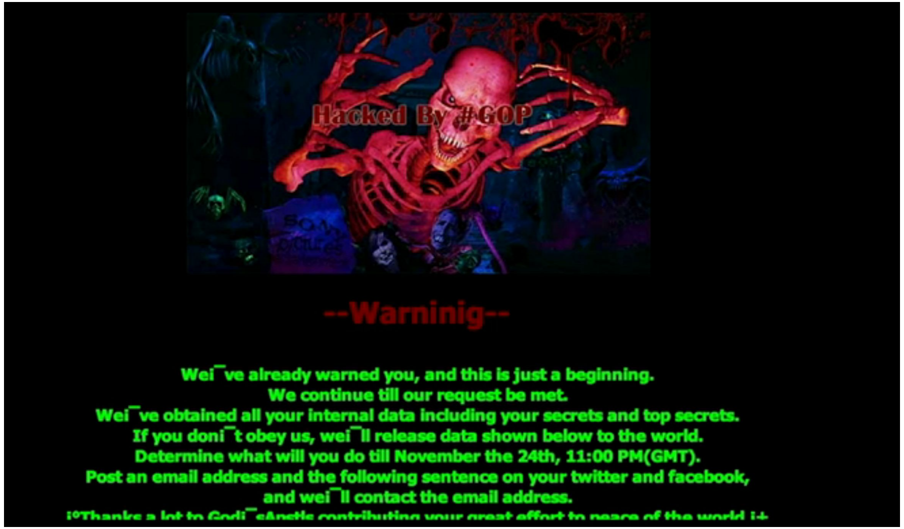
(slide credits: Kirill Nikitin)

Outline

- Organizational Network Security Practices
- Virtual Private Network (VPN)
- Securing Network Perimeter
    - Firewalls
    - Intrusion Detection Systems
- Logging and Backups

Security Breach at Sony (2014)

- The attack included a listening implant, backdoor, proxy tool, destructive hard drive and target cleaning tools.
- Hackers stole and released to the public: pre-release movies, people's private information, and sensitive documents.
- Hackers demanded Sony to pull the movie, The Interview - a comedy about a plot to assassinate North Korean leader Kim Jong-un.



Hacked By #GOP

--Warninig--

Wei¯ve already warned you, and this is just a beginning.
We continue till our request be met.
Wei¯ve obtained all your internal data including your secrets and top secrets.
If you doni¯t obey us, wei¯ll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Post an email address and the following sentence on your twitter and facebook,
and wei¯ll contact the email address.
i°Thanks a lot to Godi¯sApstls contributing your great effort to peace of the world i±

Security Breach at Target (2014)

Credit: Bloomberg

- Malware installed in Target’s security and payments system, stealing details of every credit card used at the company’s 1,797 U.S. stores.
- Security alerts on Dec 2, 2014. Target reacts only in two weeks.
- Result: 40 millions credit card numbers stolen.

Organizational Network Security Practices

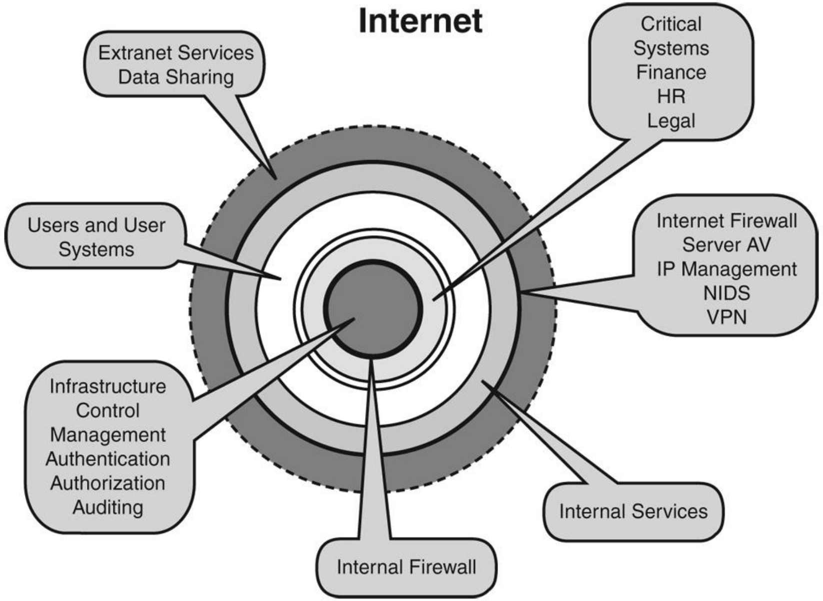
- Network compartmentalization
  - Demilitarized Zone (DMZ): exposes organization’s external facing networks to untrusted networks
  - Virtual Local Area Networks (VLANs): network partitioning at layer 2, for different uses inside a company’s network
- Secure communication over external network (TLS, IPSec)
- Commercial global WAN solutions, e.g., Aryaka, to connect branch offices and SaaS applications, or accelerate applications on-premises

Network Compartmentalization

- Break down the network into segments based on system and data classification or into functional zones
- Access from zone to zone can be managed by access control lists (ACLs) in routers or firewalls
- Mainly addresses two points:
  - Prevents all-at-once compromise of facilities
  - Perimeter defense protects the data center from external threats with little protection against internal threat agents

Network Compartmentalization - Architecture

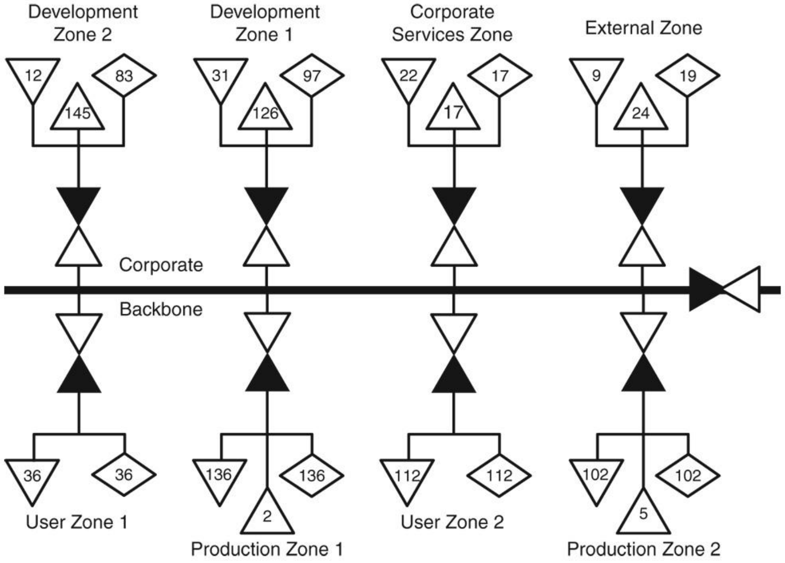
- In classic concentric architecture, access rights to services increase with each level, moving between levels managed by access control
- In Windows, the controls are enforced using Active Directory (AD) and Lightweight Directory Access Protocol (LDAP). In Unix, it is done with Access Control Lists (ACL).
- The downside is significance of potential damage if anti-virus is bypassed



Credit: NetworkWorld

Network Compartmentalization - Architecture

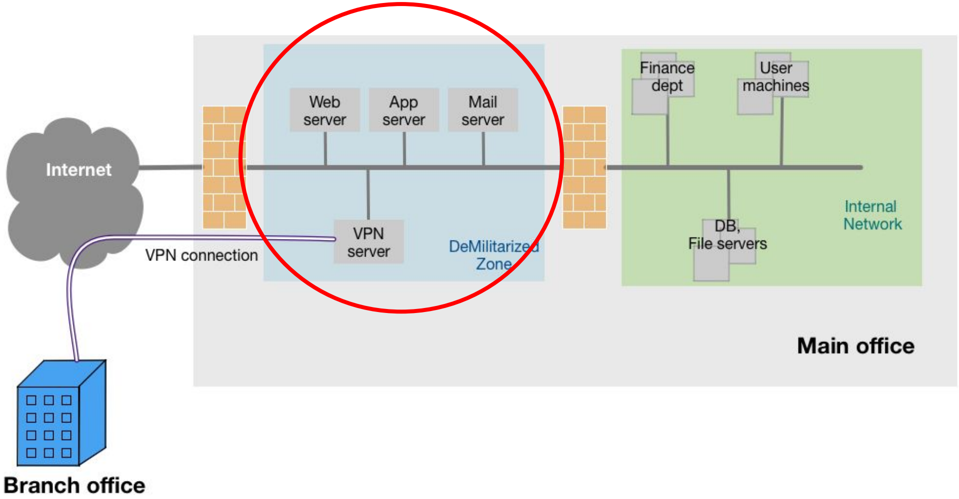
- Creating containment zones aims at stopping viruses from spreading between zones
- Communication between zones goes through firewalls
- The difficulty is creating firewall rules for each case -> easy to make mistakes



Credit: NetworkWorld

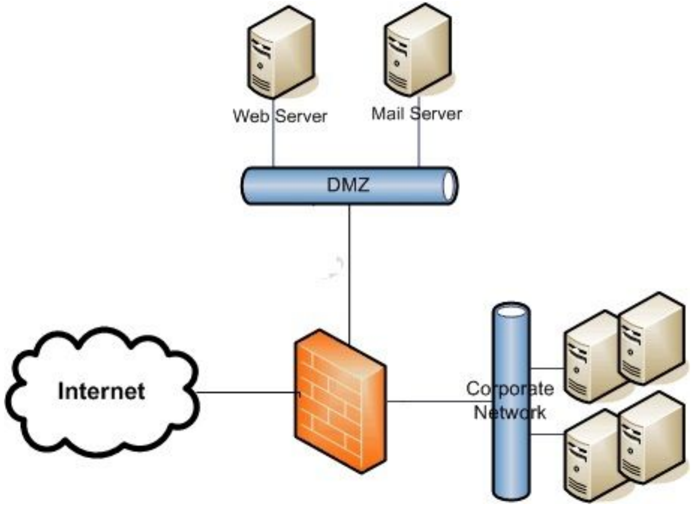
Demilitarized Zone (DMZ)

- A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, e.g., Internet.
- An external network node can access only what is exposed in the DMZ
- The most common services in DMZ are web, email, DNS, and FTP servers

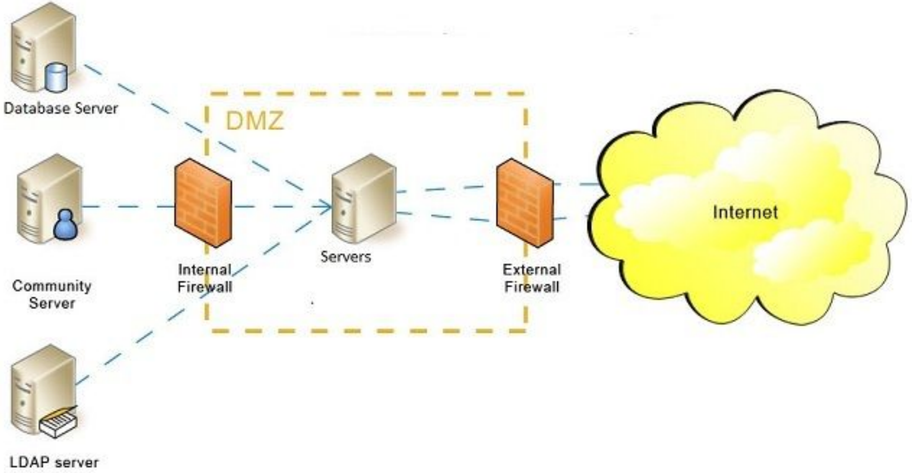


Demilitarized Zone (DMZ)

Two common architectures



Single firewall



Dual firewall

Credit: Mrinal Srivastava. DMZ

Virtual Local Area Networks (VLANs)

- A Virtual LAN is a partitioned or isolated broadcast domain inside a bigger network. The partitioning is done at the data link layer and often configured on switches.
- Membership can be by port on a bridge, MAC addresses of clients or type of a protocol running above data link layer.
- Network segmentation with virtual local area networks (VLANs) creates a collection of isolated networks within an organization

Virtual Local Area Networks (VLANs)

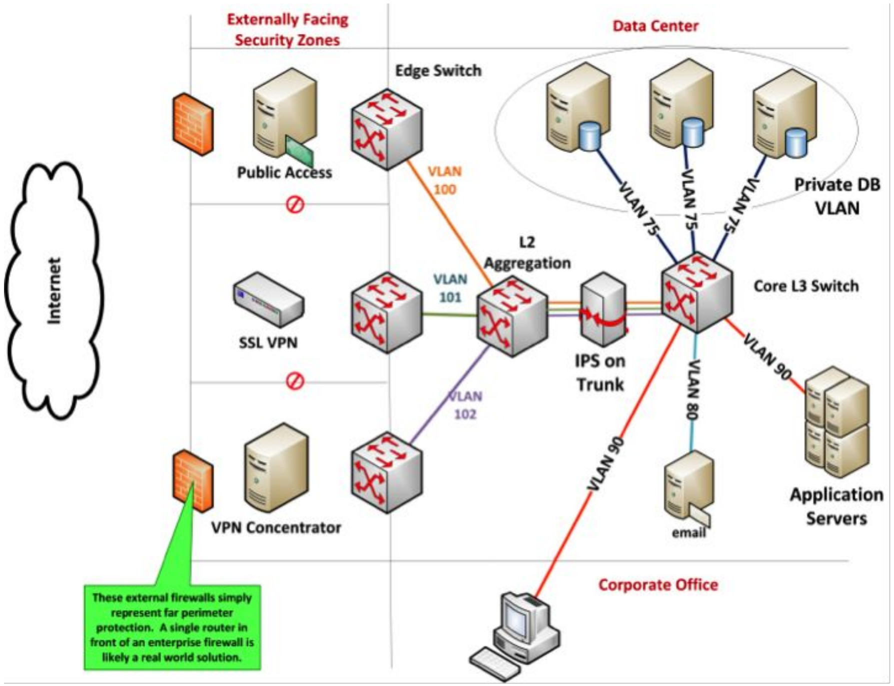
What do “isolated networks” provide?

- Authorized users can “see” only their network segment.
- Possibility to run different protocols in different network segment and limit packet circulation.
- It enables secure, flexible user mobility: with 802.1x, a RADIUS server or AD can assign the appropriate VLAN dynamically to a user or device.

Virtual Local Area Networks (VLANs)

Possible setup for an organization

The backbone switches are the ones that are supposed to tag the messages, therefore keeping the VLANs separated



These external firewalls simply represent far perimeter protection. A single router in front of an enterprise firewall is likely a real world solution.

Credit: InfoSec Institute

VLAN Attacks

VLAN MAC Flooding is an overflow of a switch routing table containing port/MAC address/VLAN assignments.

- A packet without address information in the table causes the switch to perform an ARP broadcast to determine the port through which to send the packet.
- An attacker continuously sends a large number of spoofed MAC addresses to the switch filling routing table.
- If the table fills up, all incoming packets are sent out all ports: regardless of VLAN assignment, effectively turning the switch into a hub -> attacker sees all/most packets.

Defense

- Manually bind MAC addresses to each port or configure the switch to learn the first *n* MAC addresses; or use 802.1x to force packet filtering.

VLAN Attacks

VLAN Hopping enables traffic from one VLAN to be seen by another VLAN.

Switch Spoofing

- An attacker takes advantage of incorrectly configured switch ports. The default configuration of the switch port is dynamic auto. The network attacker configures a system to spoof itself as a switch by emulating config messages and forming a trunk with a legitimate switch.

- A defense is to disable auto port trunking (switch-to-switch connection) and set it manually.

VLAN Attacks

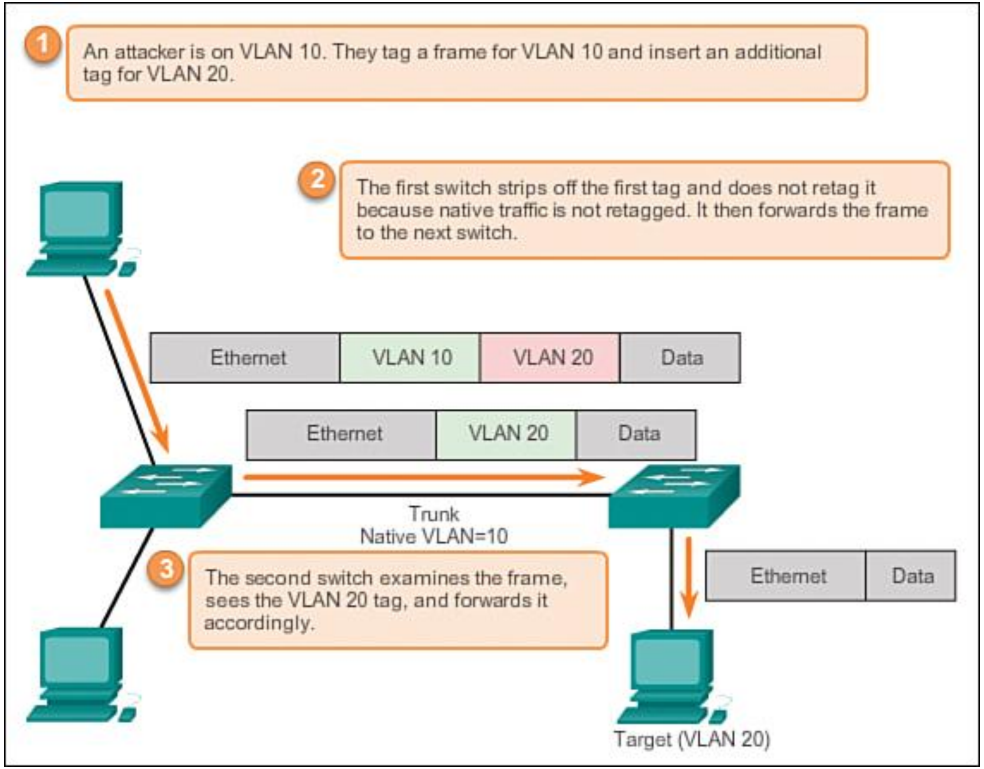
VLAN Hopping enables traffic from one VLAN to be seen by another VLAN.

Double tagging

- Most switches perform only one level of 802.1Q de-encapsulation, which allows an attacker to embed a hidden 802.1Q tag inside the frame. This tag allows the frame to be forwarded to a VLAN that the original 802.1Q tag did not specify (see fig. in the next slide).

- A defense is to ensure that the native VLAN of the trunk ports is different from the VLAN of any user ports.

Double Tagging Attack



1. An attacker is on VLAN 10. They tag a frame for VLAN 10 and insert an additional tag for VLAN 20.

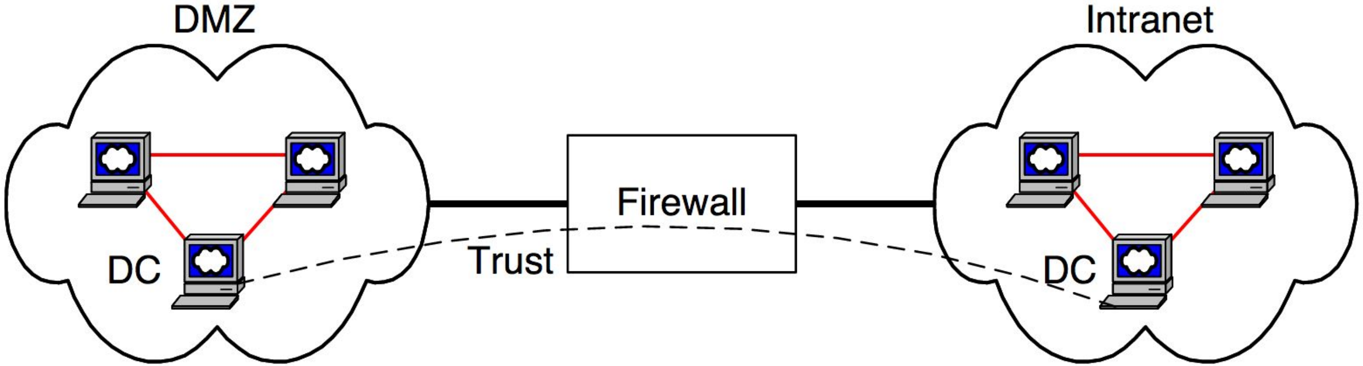
2. The first switch strips off the first tag and does not retag it because native traffic is not retagged. It then forwards the frame to the next switch.

3. The second switch examines the frame, sees the VLAN 20 tag, and forwards it accordingly.

Credit: Cisco Press

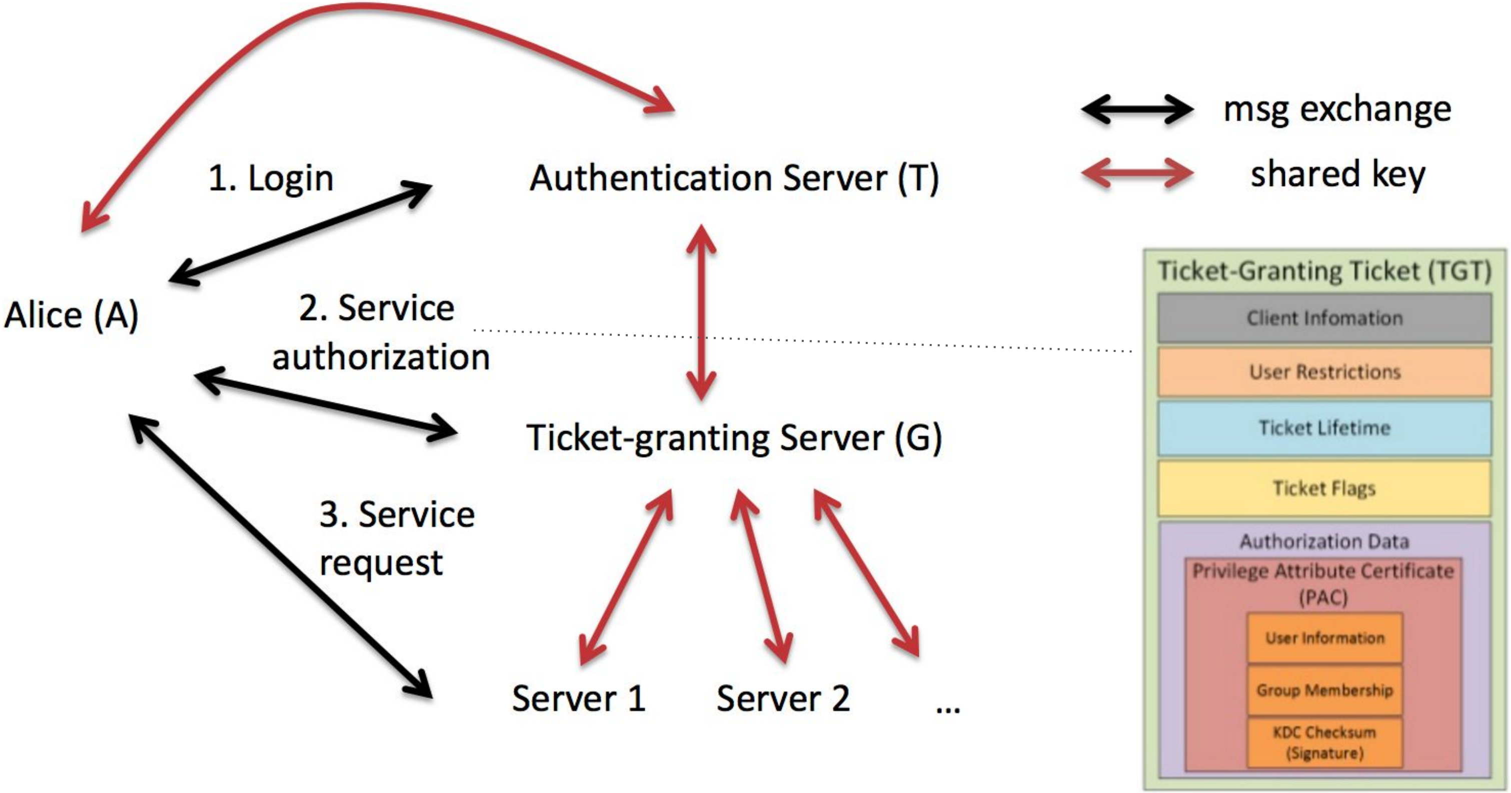
Active Directory (AD)

- Directory service that Microsoft developed for Windows domain networks.
- Domain Controller (DC) authenticates and authorizes users.
- Domains in AD correspond to VLANs.
- Basic architecture with one DC in DMZ and one in intranet, separated by a firewall:



Credit: Microsoft White Paper

Review: Kerberos Architecture



Slide adapted from Information Security course at ETH, ©Srdjan Capkun

Attack Example on Active Directory (AD)

Exploiting an unpatched Domain Controller via Kerberos vuln. (MS14-068)

- Request a Kerberos TGT authentication ticket without a PAC as a standard user, the DC replies with the TGT (with no PAC which usually contains group membership, this is unusual).
- Generate a forged PAC, without a key, so the generated PAC is “signed” with plain MD5 instead of HMAC_MD5 using the domain user’s password data.
- Send the PAC-less TGT to the DC with the forged PAC as Authorization-Data as part of a TGS service ticket request.
- The DC seems to be confused by this, so it discards the PAC-less TGT sent by the user, creates a new TGT and inserts the forged PAC in its own Authorization-Data, and sends this TGT to the user.
- This TGT with the forged PAC enables the user to be a Domain Admin on vulnerable DCs.

Gavin Millard @gmillard · 11h

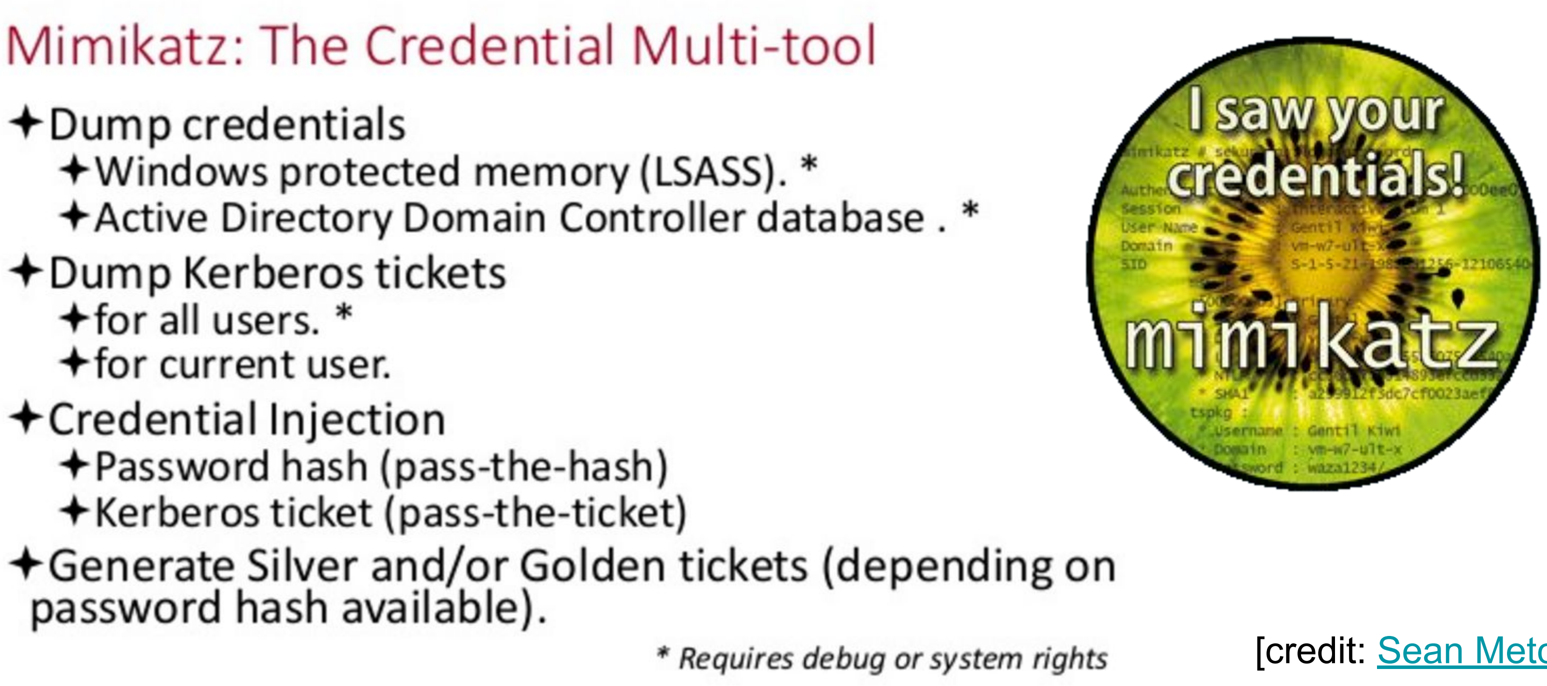
MS14-068 in the real world.

"Welcome Captain. Would you like a coffee before you take off"

#infosec

One of many Active Directory attacks

With many well-developed exploit tools and practices available...



Mimikatz: The Credential Multi-tool

- ✦Dump credentials
  - ✦Windows protected memory (LSASS). *
  - ✦Active Directory Domain Controller database . *
- ✦Dump Kerberos tickets
  - ✦for all users. *
  - ✦for current user.
- ✦Credential Injection
  - ✦Password hash (pass-the-hash)
  - ✦Kerberos ticket (pass-the-ticket)
- ✦Generate Silver and/or Golden tickets (depending on password hash available).

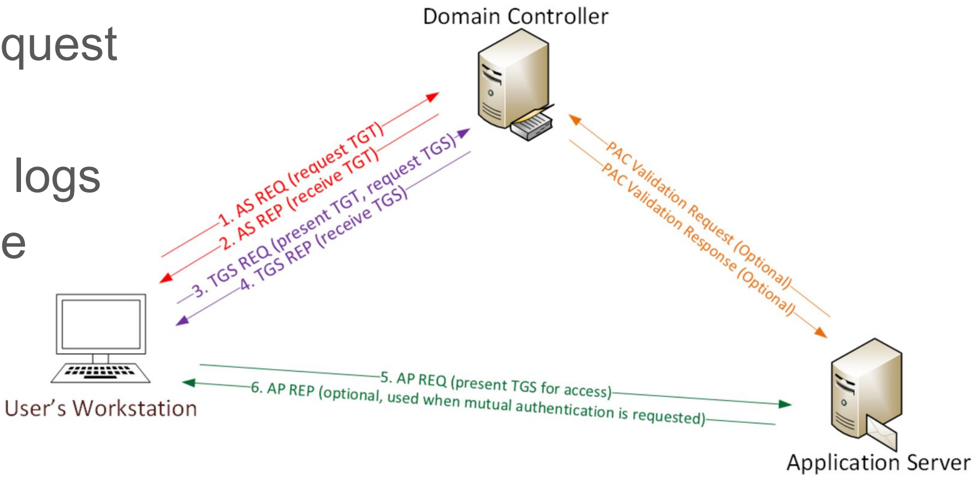
** Requires debug or system rights*

[credit: Sean Metcalf]

Kerberos is never sending a plain text pwd over the nw, not even the hash of the pwd. What it sends over the nw is the HMAC, but still there's the limitation here explained. The HMAC is based on a pwd

Example 2: Kerberoast password cracking

- Any user with a valid TGT can request a TGS for a Kerberos service
- DC doesn’t check if user actually logs into or even has access to service
- DC just validates TGT, produces corresponding TGS
- That TGS is encrypted with service’s private symmetric key, often derived from a 10-12 character password. (See the problem?)
- Attacker can Kerberoast that key, without even interacting with service first


Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User’s Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

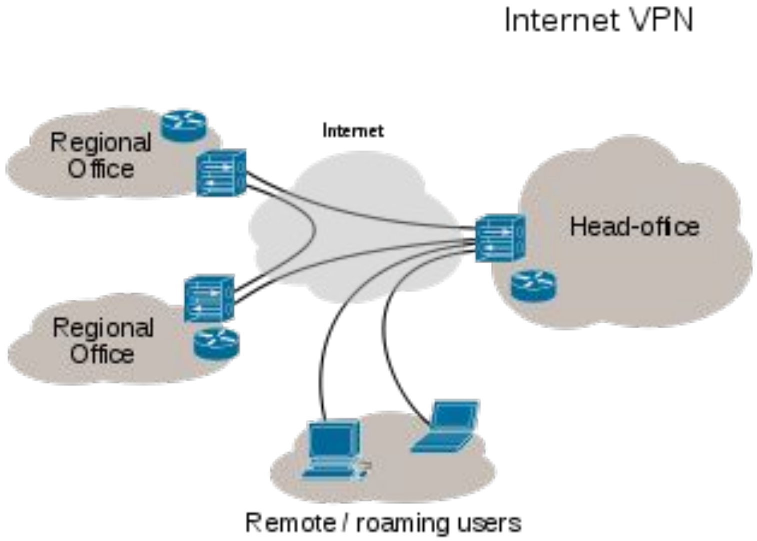
[credit: Sean Metcalf]

Outline

- Organizational Network Security Practices
- **Virtual Private Network (VPN)**
- Securing Network Perimeter
    - Firewalls
    - Intrusion Detection Systems
- Logging and Backups

Virtual Private Network (VPN)

- VPN is an extension of a private network across a public network, such as the Internet.
- A virtual topology is built on an existing, shared physical network infrastructure.



Credit: Wikipedia. Virtual Private Network

Types of VPN Services

1. Local Area Network (LAN) Interconnect VPN services
   - interconnects local area networks located at multiple geographic areas.
2. Dial-up VPN services
   - supports mobile and telecommuting employees in accessing the company's Intranet from remote locations.
3. Extranet VPN services
   - combines 1 and 2. This infrastructure enables external entities to access specific areas of the company's Intranet. The allowed specific area is denoted as the Demilitarized Zone (DMZ).

Credit: Venkateswaran, Ramachandran. "Virtual private networks." IEEE potentials 20.1 (2001): 11-15.

VPN Implementations

layer 3 VPN

Network Layer VPNs (IPsec, MPLS, …)

- Usually implemented with a tunnel connecting two points of a VPN across the shared network infrastructure.
- The network layer packets leaving a VPN node at one end of the tunnel are appended with an additional IP header whose destination address reflects the other end where the additional header is stripped out.

Link Layer VPNs (L2TP, VPLS, PW, …)

- The links belonging to the VPNs are implemented as virtual link-layer circuits.
- Often does not provide confidentiality by itself, but relies on an encryption protocol that it passes within the tunnel.

Outline

- Organizational Network Security Practices
- Virtual Private Network (VPN)
- **Securing Network Perimeter**
  - Firewalls
  - Intrusion Detection Systems
- Logging and Backups

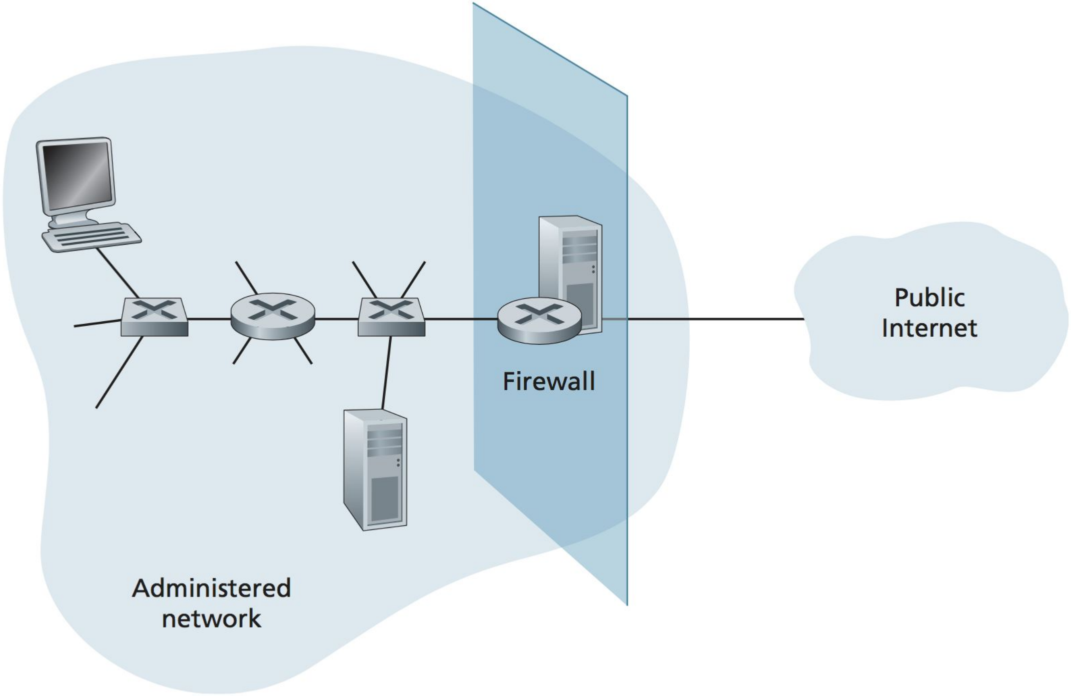
Securing Network Perimeter

Why?

- Restrict access to internal resources for machines outside corporate network
- Hide internal network structure
- Prevent employers from accessing malicious websites

Firewalls

Filters both incoming and outgoing traffic



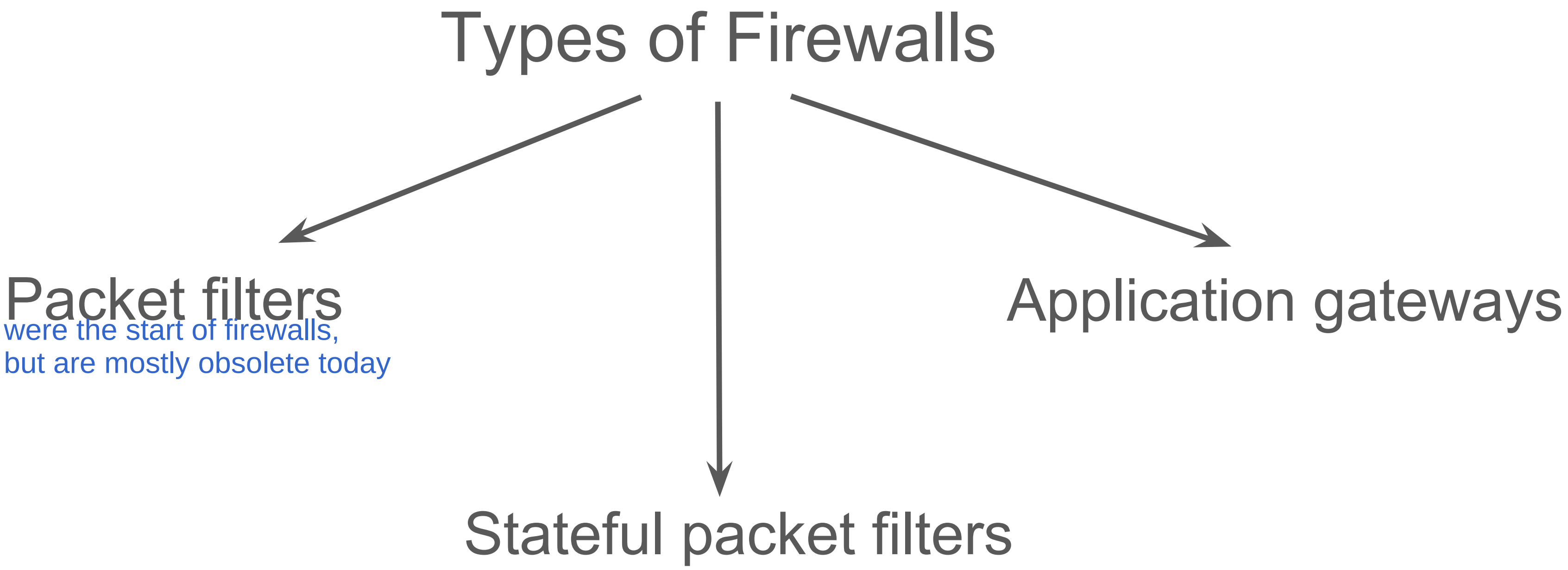
Credit: J. Kurose, K. Ross. *Computer Networking: A Top-Down Approach (6th Edition)*

Firewalls

Design criteria:

1. All traffic from outside to inside, and vice versa, passes through the firewall
2. Only authorized traffic, as defined by the local security policy, is allowed to pass
3. Firewall itself is (hopefully) immune to penetration

Firewalls



Types of Firewalls

Packet filters

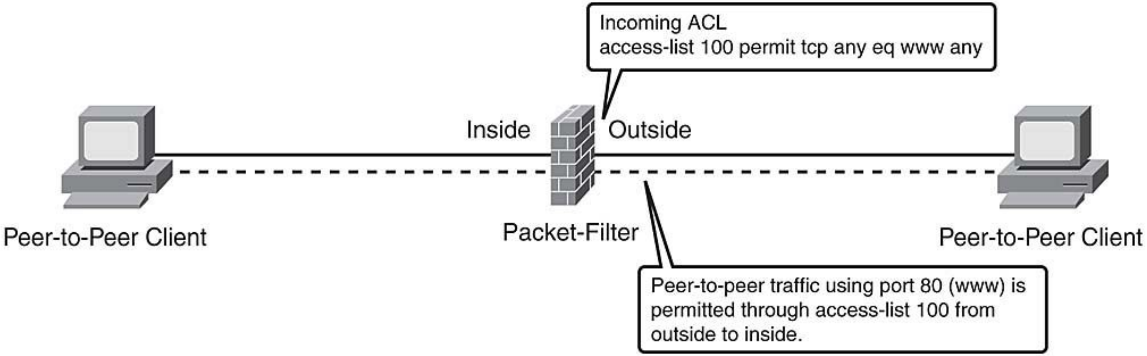
were the start of firewalls,
but are mostly obsolete today

Application gateways

Stateful packet filters

Packet Filters

- Examining each data datagram in isolation based on: IP addresses, transport protocol, ports, TCP flags.
- Not concerned with packet data
- Examples:
  - ○ drop all SYN packets
  - ○ drop outgoing packets using port 80 (HTTP)



Incoming ACL
access-list 100 permit tcp any eq www any
Inside
Outside
Peer-to-Peer Client
Packet-Filter
Peer-to-Peer Client
Peer-to-peer traffic using port 80 (www) is permitted through access-list 100 from outside to inside.

Credit: NetworkWorld. Chapter1: Types of Firewalls

Packet Filters

Advantages:

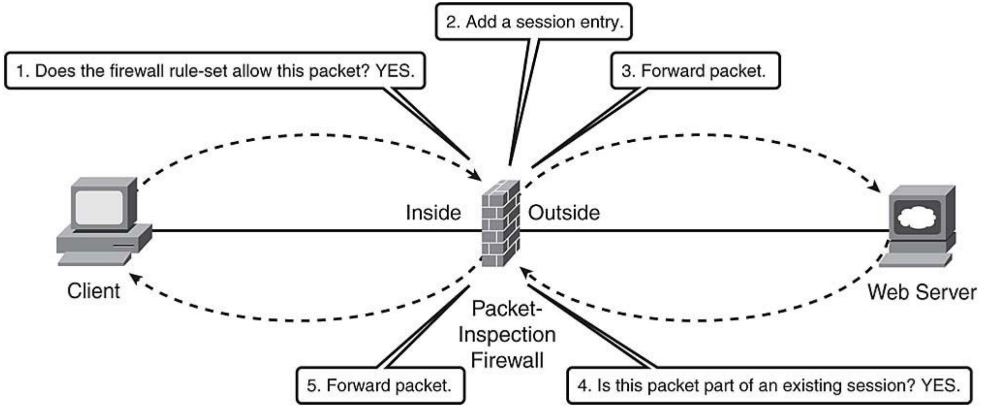
- ✓ Can be easily located in about every device on the network (routers, switches, etc.)
- ✓ Fast deployment

Caveats:

- × Can be tricked by spoofed IP addresses
- × No data validation
- × Can be tricked by packet fragmentation

Stateful Packet Filters

- In addition to datagrams in isolation, track a connection state
- Block packets deviating from standard behaviour (e.g., out of sequence)
- State table for each connection (cleaned up after timeout)
  - For example, track TCP handshake and accept TCP ACK only after seeing SYN and SYN-ACK



1. Does the firewall rule-set allow this packet? YES.
2. Add a session entry.
3. Forward packet.
Inside
Outside
Client
Web Server
Packet-Inspection Firewall
4. Is this packet part of an existing session? YES.
5. Forward packet.

Credit: NetworkWorld. Chapter1: Types of Firewalls

Stateful Packet Filters

Advantages:

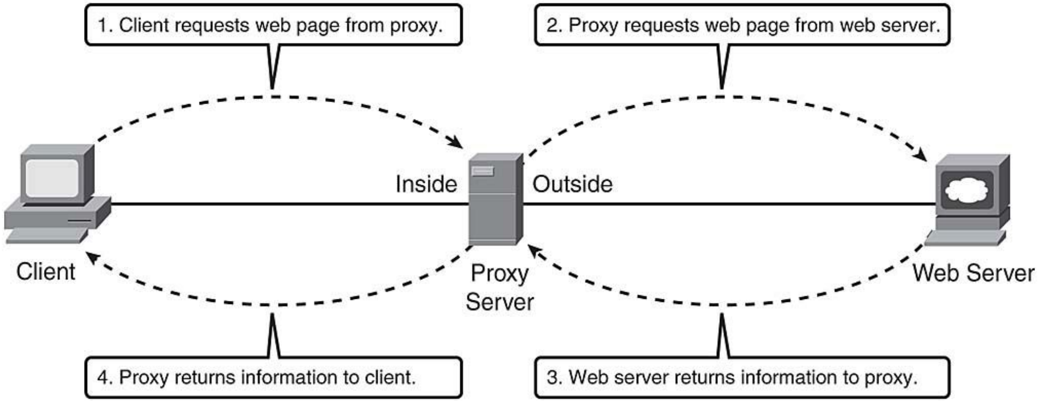
- ✓ Inexpensive improvement over packet filters
- ✓ Offer deep packet inspection

Caveats:

- × Does not help with UDP
- × Still cannot stop application-level attacks

Application Gateways

- Splices and relays application-specific requests and responses
- Gateway is application-aware so can look inspect packet data, e.g., detect emails with executable files
- Common examples:
  - HTTP proxy server
  - Telnet gateway


1. Client requests web page from proxy.
2. Proxy requests web page from web server.
Inside
Outside
Client
Proxy Server
Web Server
4. Proxy returns information to client.
3. Web server returns information to proxy.

Credit: NetworkWorld. Chapter1: Types of Firewalls

Application Gateways

Advantages:

- ✓ Additional "buffer" from port scans and application attacks
- ✓ Can authenticate users

Caveats:

- × Application-awareness has to be configured for custom applications
- × Potential interference with the application
- × Slower than packet filters

Problems with Firewalls

- Software bugs
- Does not prevent insider attacks
- Running one protocol on top of another (e.g., IP over HTTP)
- Firewall is only as effective as configured rules

HAVE YOU BEEN WORKING ON YOUR CHRISTMAS LIST?
DONE, AND DONE
JIM DAVIS 12-14
www.garfield.com
I ALREADY E-MAILED IT TO SANTA
Distributed by Universal Uclick
HE GOT THROUGH THE FIREWALL AGAIN, SIR
MAN, THAT CAT CAN HACK

Intrusion Detection Systems (IDSs)

- An IDS performs deep packet inspection for **ALL** applications to detect potential intrusion
  - Generates alerts if deems traffic is suspicious
  - Intrusion Prevention System (IPS) → filters such traffic out
- Two technologies:
  - Signature-based systems
  - Anomaly-based systems
- Possible issues:
  - False positives
  - False negatives

SpeakUp - MM88 fever is a rare fatal disease, only 10 in 1 million people have it. You take a test and it comes out positive. The test has a small false positive rate of 0.1%. What is the probability that you actually have the disease?

A	10%
B	99.9%
C	1%
D	50%

Signature-based Systems

- Network traffic is examined for preconfigured and predetermined attacks patterns
- IDS compares every packet with signatures from a pattern database
- Possible issues:
  - Require previous knowledge of an attack to generate an accurate signature -> hard to catch unknown attacks
  - Matched signature does not always mean attack *(i.e., false alarms)*
  - A lot of signatures -> system can be overwhelmed with processing
- Signature examples:
  - High number of failed login attempts
  - Attempts to sign in with SQL-like names
- ***Snort*** is an example of open-source IDS & IPS

Credit: Huffington Post

Anomaly-based Systems

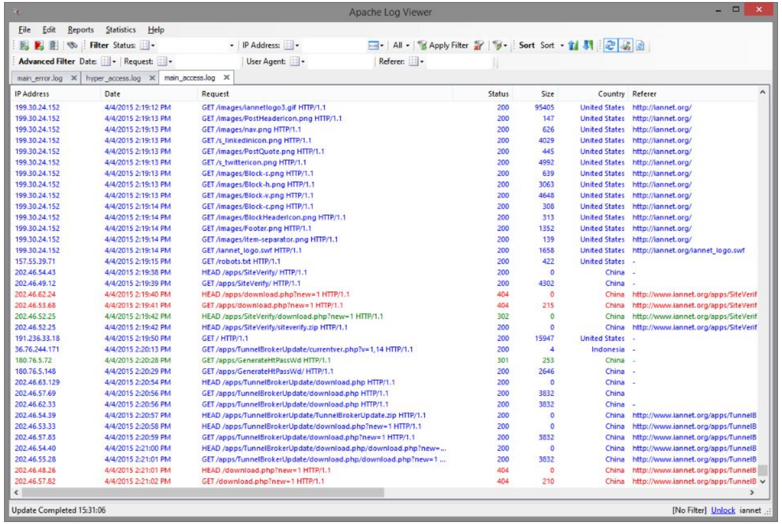
- IDS creates a traffic profile during normal operation to calibrate
- During monitoring, it looks for statistically unusual packet streams
  - *e.g.*, growth in port scans or ping sweeps
- Can potentially detect new undocumented attacks
- Hard to distinguish normal traffic and statistically different -> false positives and false negatives
- Hot application for machine learning techniques

Outline

- Organizational Network Security Practices
- Virtual Private Network (VPN)
- Securing Network Perimeter
  - Firewalls
  - Intrusion Detection Systems
- **Logging and Backups**

Logging

- Important for identifying security incidents, monitoring policy violations, non-repudiation control
- Some sources of event data
  - Firewalls and IDS
  - Client machines
  - Database applications



IP Address	Date	Request	Status	Size	Country	Referer
199.30.24.152	4/4/2015 2:19:12 PM	GET /images/iannetlogo3.gif HTTP/1.1	200	95405	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/PostHeaderIcon.png HTTP/1.1	200	147	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/nav.png HTTP/1.1	200	626	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /s_linkedinicon.png HTTP/1.1	200	4029	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/PostQuote.png HTTP/1.1	200	445	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /s_twittericon.png HTTP/1.1	200	4992	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/Block-s.png HTTP/1.1	200	639	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/Block-h.png HTTP/1.1	200	3063	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/Block-v.png HTTP/1.1	200	4648	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /images/Block-c.png HTTP/1.1	200	308	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /images/BlockHeaderIcon.png HTTP/1.1	200	313	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /images/Footer.png HTTP/1.1	200	1352	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /images/item-separator.png HTTP/1.1	200	139	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /iannet_logo.swf HTTP/1.1	200	1658	United States	http://iannet.org/iannet_logo.swf
157.55.39.71	4/4/2015 2:19:15 PM	GET /robots.txt HTTP/1.1	200	422	United States	-
202.46.54.43	4/4/2015 2:19:38 PM	HEAD /apps/SiteVerify/ HTTP/1.1	200	0	China	-
202.46.49.12	4/4/2015 2:19:39 PM	GET /apps/SiteVerify/ HTTP/1.1	200	4302	China	-
202.46.62.24	4/4/2015 2:19:40 PM	HEAD /apps/download.php?new=1 HTTP/1.1	404	0	China	http://www.iannet.org/apps/SiteVerif
202.46.53.68	4/4/2015 2:19:41 PM	GET /apps/download.php?new=1 HTTP/1.1	404	215	China	http://www.iannet.org/apps/SiteVerif
202.46.52.25	4/4/2015 2:19:42 PM	HEAD /apps/SiteVerify/download.php?new=1 HTTP/1.1	302	0	China	http://www.iannet.org/apps/SiteVerif
202.46.52.25	4/4/2015 2:19:42 PM	HEAD /apps/SiteVerify/siteverify.zip HTTP/1.1	200	0	China	http://www.iannet.org/apps/SiteVerif
191.236.33.18	4/4/2015 2:19:50 PM	GET / HTTP/1.1	200	15947	United States	-
36.76.244.171	4/4/2015 2:20:13 PM	GET /apps/TunnelBrokerUpdate/currentver.php?v=1,14 HTTP/1.1	200	4	Indonesia	-
180.76.5.72	4/4/2015 2:20:28 PM	GET /apps/GenerateHtPassWd HTTP/1.1	301	253	China	-
180.76.5.148	4/4/2015 2:20:29 PM	GET /apps/GenerateHtPassWd/ HTTP/1.1	200	2646	China	-
202.46.63.129	4/4/2015 2:20:54 PM	HEAD /apps/TunnelBrokerUpdate/download.php HTTP/1.1	200	0	China	-
202.46.57.69	4/4/2015 2:20:56 PM	GET /apps/TunnelBrokerUpdate/download.php HTTP/1.1	200	3832	China	
202.46.62.33	4/4/2015 2:20:56 PM	GET /apps/TunnelBrokerUpdate/download.php HTTP/1.1	200	3832	China	-
202.46.54.39	4/4/2015 2:20:57 PM	HEAD /apps/TunnelBrokerUpdate/TunnelBrokerUpdate.zip HTTP/1.1	200	0	China	http://www.iannet.org/apps/TunnelB
202.46.53.33	4/4/2015 2:20:58 PM	HEAD /apps/TunnelBrokerUpdate/download.php?new=1 HTTP/1.1	200	0	China	http://www.iannet.org/apps/TunnelB
202.46.57.83	4/4/2015 2:20:59 PM	GET /apps/TunnelBrokerUpdate/download.php?new=1 HTTP/1.1	200	3832	China	http://www.iannet.org/apps/TunnelB
202.46.54.40	4/4/2015 2:21:00 PM	HEAD /apps/TunnelBrokerUpdate/download.php/download.php?new=...	200	0	China	http://www.iannet.org/apps/TunnelB
202.46.55.28	4/4/2015 2:21:01 PM	GET /apps/TunnelBrokerUpdate/download.php/download.php?new=1 ...	200	3832	China	http://www.iannet.org/apps/TunnelB
202.46.48.26	4/4/2015 2:21:01 PM	HEAD /download.php?new=1 HTTP/1.1	404	0	China	http://www.iannet.org/apps/TunnelB
202.46.57.82	4/4/2015 2:21:02 PM	GET /download.php?new=1 HTTP/1.1	404	210	China	http://www.iannet.org/apps/TunnelB

Update Completed 15:31:06

[No Filter] Unlock iannet

Credit: Apache Logs Viewer

Logging

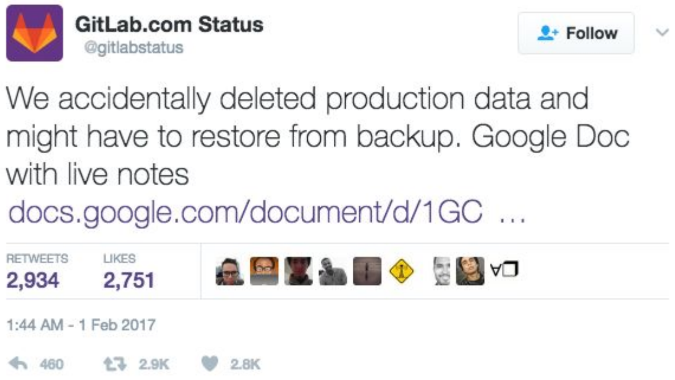
SpeakUp - What events should _NOT_ be logged?

A	Authentication attempts
B	Text editor crashes
C	Session management failures
D	Input validation failures

Logging

- What to log?
  - Input and output validation failures *(e.g., invalid parameter values or invalid data encoding)*
  - Authentication and authorization successes and failures
  - Session management failures *(e.g., cookie session identification value modification)*
  - Application errors and system events
  - Use of higher-risk functionality *(e.g., addition or deletion of users, changes to privileges)*
- What not to log?
  - Access tokens, authentication passwords, and encryption keys
  - Personal user data that is illegal to collect

Backups



GitLab.com Status
@gitlabstatus

We accidentally deleted production data and might have to restore from backup. Google Doc with live notes docs.google.com/document/d/1GC …

RETWEETS 2,934 LIKES 2,751

1:44 AM - 1 Feb 2017

460 2.9K 2.8K

Source: GitLab Status Twitter

Example: GitLab

Events timeline:

- 2017/01/31 **6pm UTC**: Spammers are hammering GitLab’s database, causing a lockup.
- 2017/01/31 **10pm UTC**: DB replication effectively stops.
- 2017/01/31 **11pm-ish UTC**: *team-member-1* starts removing db1.cluster.gitlab.com by accident.
- 2017/01/31 **11:27pm UTC**: *team-member-1* terminates the removal but 300 GB of data is lost.
- They figure out that regular backups are only done once every 24 hours, and some system parts are not backed up at all.
- **GitLab manages to restore from a six-hour-old backup but loses all the data submitted after.**

Backups

- Backup types:
  - Full
  - Incremental - only contains all the data that has changed since **any** previous backup
  - Differential - contains all the data that has changed since the previous **full** backup
- The 3-2-1 rule: at least 3 copies of data, stored on at least 2 different media, and at least 1 of the copies must be stored offsite
- Should backups be encrypted?

Credit: Reference.com

Conclusion

- Designing enterprise network architecture is integral to securing operations
- Securing the enterprise involves various techniques:
    - Compartmentalization, isolation, access control
    - Securing the network parameter
        - Control the outgoing/incoming traffic
        - Firewalls are the traditional tools
        - More advanced tools available: IDS, IPS, stateful packet filters
- Always have backups!
- Logging is invaluable for monitoring operations and diagnostics