William Prado
05/08/2025

YTB-IBM Cloud

Module = 101

Identity & Access Management (IAM)

IAM

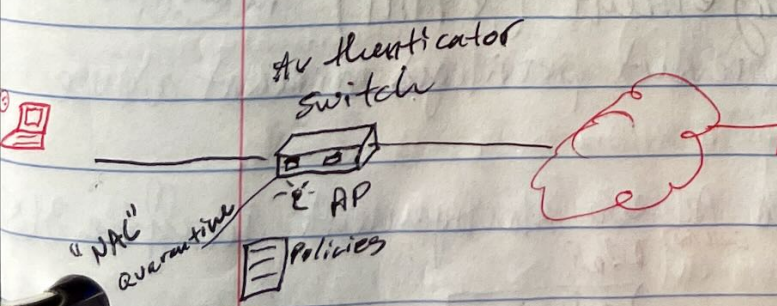
Identify (Claim)
Authentication (prove claim
Authorization (rights + privileges)
Accounting (logging, Auditing)

Identity & Access Management

[A]dmin - Idm Prov/De prov
A uthn - who?] am
A uthz - allowed]
A udit

Authenticates Client + Network Access
Network Acess Control
802.1x - Port Base Acess Control
Switch + Acess Point
EAP - Extended Authentication Protocol ≅ API

- PKI - certificate
- Kerberos - tickets
- Radius/TACACS
- LDAP/AD



LDAP port 389 unsecure, LDAP port 636 secure

William Prado
05/08/2025
Module 10.2

Authorization & Access Control.

YTB. What is discretionary Access Control.

DAC
- owner of a resource decides how it is shared.
- each resource has an owner (the creator). & who has access.

YTB - Discretionary Access Control.

DAC owner of a resource decides how it can share.

YTB - Role Based Access Control (RBAC)

User → Role → Rights

Enterprise setting, access may be based on job role.

role: sets of rights / permissions.

Difference btw RBAC & DAC

RBAC = Access based on the role you have

DAC = Access based on ownership

Privileged Access Management (PAM) Checks & Balances For root & admin

Control elevated access prevent privileged account abuse

YTB - Introducing Privileged Access Management in office 365

Approval group

admin

Zero Standing Access

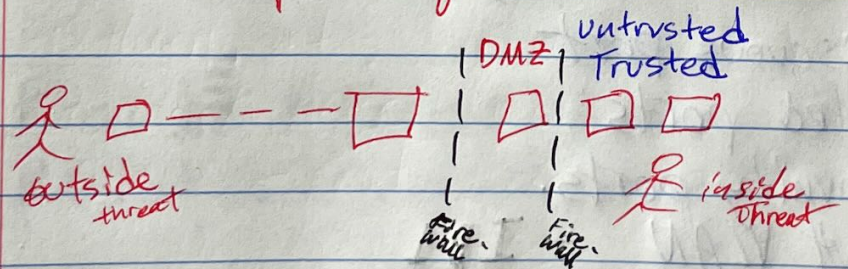
William Prado
05/08/2025

What is privilege escalation?

Least privilege - granting just enough rights to perform their job & no more.

Separation of Duties - establish checks & balances against possibility that critical systems or procedures can be compromised by insider threats. Devide tasks prevents ethical conflicts or abuse of power.

IBM YTB Zero Trust - Why Implement Zero Trust
- Assume Breach
- Verify - Trust
- least privilege



Module 10.3 Perimeter- Focus vs. Defense in Depth

Perimeter security

Defense in Depth
- Application & Data Security
- Host Security
- Network security
- Physical security
- Policies & Procedures

Review Port ~~#~~ ...
Access Control List ... Filters.
Firewall ... Filter

William Prado
05/08/2025

10.4

Perimeter Sec. vs Endpoint Sec.

- Disable unneeded switchports
- Configure protection mechanisms
- MAC Filtering
- Dynamic ARP Inspection
- DHCP Snooping
- Neighbor Discovery (ND) Inspection & Router Advertisement (RA) Guard.
- Port Security (IEEE 802.1X Port Based Network Access Control) Authentication Devices > wired/wireless > must authenticate before being allowed access to switch port & port being turned on.

VLAN & PVLAN Best Practices.

VLAN - recap

Private VLAN (PVLAN)

Promiscuous port

Isolated ports

Community ports.

Default VLAN = ID 1

Native VLAN untagged traffic.

Network access control (NAC) system to authenticate/authorize access to a network

Switch - connects/mngs communications on a network.

Switch ports dedicated interface on a switch that connects devices.

Port Security > Secure physical access > Regularly update switch firmware > Disable unneeded ports > Configure MAC filtering > Enable Router Advertisement Guard (RA) > Configure DHCP Snooping > Implement 802.1x authentication (EAP).

William Prado
05/08/2025

ACL permit or deny
Review ports
Firewall – Filter
Stateless vs. StateFull
UTM vs NGFW
HWD v SFTW
Proxy Server vs NAT "Application"

Review 10%

Access control: only authorized users & devices can access resources (physical & digital measures).

Defense in depth: layers of security (policies & mechanisms) safeguard data integrity, confidentiality, and availability.

Firewalls & Proxies: filter traffic & manage requests for network security & performance.

Content Filtering: Fine-tune traffic w/ rules based on protocols, addresses, content, and more.

Lab: 9.2.5 Note: tcp.flags.syn==1
flag: 0x002
terminal: hping3 192.168.10.19

Lab: 9.2.6 tcp.flags.syn==1 and tcp.flags.ack==0