Authentication

Monitoring and Log Management

AAA

- Authentication is the process of verifying the identity of an entity, whether that is a person, program, or machine
- Authorization is the granting of permission to access resources, run programs, and save or change data
- Accounting is the mechanism used to create, transmit, and store records describing activity

Authentication

- Authenticating an entity can take several forms
- An entity can provide one or more of the following to demonstrate the validity of its identity claim
  - A login name or identifying string of characters, usually accompanied by a password or secret string associated with that name
  - A certificate signed by a trusted authority
  - A valid response to a challenge issued when an identity is claimed
  - Physical or virtual possession of auxiliary information such as smart cards, dongles, or one-time code generators
  - Biometric data unique to the entity when the entity is biological
  - One or more pieces of information theoretically distinct to that device, such as ethernet address
- Authenticating an entity does not grant privileges to the entity, it simply tries to establish a reasonable level of confidence that the entity is who or what they claim to be

Authorization

- Authorization is the granting of permission to perform tasks or access resources based on one or more attributes of the entity requesting authorization
- The primary attribute is the identity of the requestor, authentication precedes authorization in normal processing of requests, for situations where the identity of the requestor is relevant
- Session identifiers are often used when the authorized activity requires identification but no requestor identity is implemented
- Additional attributes may include method of access, time of access, protocols used, other parties involved, attributes of the requested resources (e.g. public web servers provide authorization to access resources based solely on protocol and resources requested, often without any authentication used)

Accounting

- Accounting for activity requires capturing information which describes the activity
- At a minimum, access accounting typically includes authentication info, authorization(s) granted, access method and location, timestamps, and when that activity changed (e.g. login/logout, change privileges, etc.)
- Accounting may include statistical or detailed data about what was done while authorization was granted, the detail level is usually related to some type of activity we are interested in summarizing such as total network traffic moved, or disk i/o caused, etc.
- When it is highly detailed to the level of specifically what was accessed, when, and the results of the access, we call it auditing, not accounting and it gets recorded differently

AAA Implementation

- Authentication, authorization, and accounting may be implemented with a single protocol by a single program or software package, or it may be split
- A non-integrated solution often amalgamates the authentication and authorization (this combo is sometimes called authortication) tasks together and serves them with a single protocol or program, while handling accounting independently or not at all, Active Directory is an example of this kind of solution
- Redundancy for performance and reliability is available with some solutions
- 3 parties are involved in AAA, the supplicant (requester), service provider (e.g. authenticator), and the AAA server

AAA Solutions

- Standalone servers provide login authentication locally, authorization by userid group membership and login shell, and accounting via tools like syslog or direct service and application logging
- Clients in small organizations typically use local per host authentication/authorization, may replicate authentication/authorization between machines, or may use distributed authentication/authorization and usually ignore accounting
- SMEs often implement only Active Directory, using centralized auth and ignoring accounting
- Larger organizations use distributed AAA solutions via servers such as Cisco Access Control Server (ACS) accessing backend AAA services for edge access, and LDAP-based solutions for user access
- Distributed AAA services are often provided by RADIUS or TACACS+ servers (Cisco solution)

Entity Definition

- A basic element of authentication is determining how to identify entities in a useful way
- Users are defined by user accounts in various ways
- Machines or devices can also be identified by name, address, network, etc.
- These identities are stored in databases which can be simple flat files like /etc/passwd and /etc/shadow (i.e. local users), distributed secure access databases such as Active Directory or LDAP (e.g. OpenLDAP), or database platforms such as MySQL/MariaDB with identity lookup programs or plugins (e.g. RADIUS servers)
- These types of identity stores and their access mechanisms are commonly referred to as directory services

OpenLDAP

- Provides an open source LDAP implementation
- Includes a server for the Directory Information Tree (DIT) and client tools to access that DIT
- Linux package name is slapd for the server and ldap-utils for the tools
- Entries to the DIT are made in LDAP Data Interchange Format (LDIF)
- Database changes are done using command line tools, or a gui frontend tool that runs those tools, webmin is a popular example

Device vs. Network

- AAA can be applied to machines (devices) as well as users
- RADIUS was designed for network edge user authentication to support dialup internet users
- TACACS was designed to support user cli authentication/authorization at a highly granular level
- Both have grown beyond these beginnings, but both still are primarily aimed at either remote connection AAA, or network device user AAA
- TACACS is typically implemented to support Cisco devices in the network, RADIUS for most other AAA situations
- Either one can use flat files, LDAP, or other directory services to provide user/machine definitions or store them in service-specific databases

AAA Sequence

- When a host or device wants access, it initiates a connection request with an access device (e.g. a switch for directly connected devices, a remote access server for remote devices, various authenticators for users)
- The authenticator sends an EAP or EAPol request to an AAA server, it may use different servers for different requests, and there are many different EAP methods for securing the communication
- The AAA server uses an authortication database to determine whether to allow access, challenge the request, or deny it
- The response is sent to the authenticator, if it is challenge, there is a further handshake
- The client may authenticate with a certificate, the server may also

FreeRADIUS

- Very popular open source RADIUS server
- Provides all aspects of AAA
- Installed as a package named freeradius
- Additional packages can link freeradius to mysql, postgresql, ldap, krb5, or AD
- Package install automatically generates the server certificate

FreeRADIUS Configuration

- Radius listens on UDP ports 1812, 1813, 1814 and 18120 by default
- Configuration is in /etc/freeradius
- radiusd.conf is the primary configuration file for the service
- clients.conf defines what authenticators can access the server and what the shared secrets are for them
- users file defines who can authenticate and what their authorizations are
- acct_users defines the accounting records to keep

Using RADIUS for Login Users

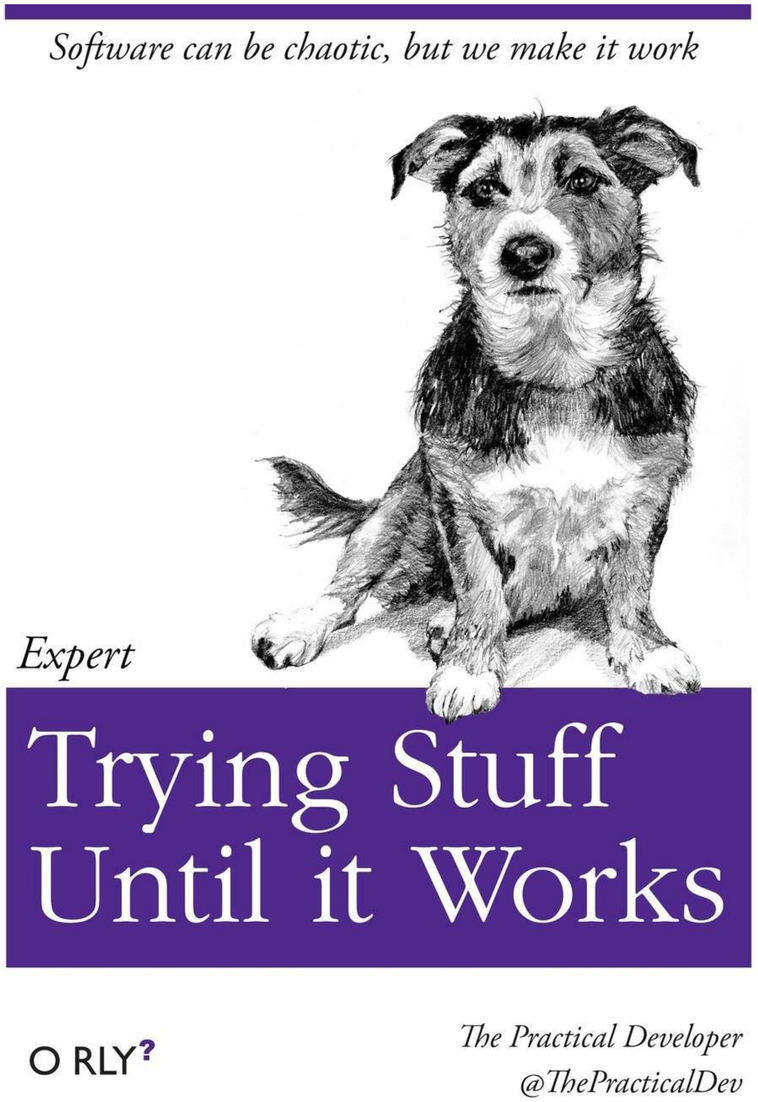
- Uncommon but illustrates using an existing RADIUS user authortication solution to provide authortication to Linux machines around a network
- Get the pam_radius module from freeradius.org and install it in /lib/security - also available as the package libpam-radius-auth
- Configure your users in the /etc/freeradius/users file
- Add pam_radius.so to the authentication methods in the /etc/pam.d/application configuration files
- Give consideration to how your RADIUS traffic is secured if your RADIUS server is not localhost (can be partially encrypted, use TLS with certificates, or tunnelled)

Using RADIUS for Network Access

- Each Network Access Server has its own configuration to set it to use Radius
- User records for network access will define the login credentials, authorized access method, and any parameters needed by the NAS or client such as VLAN numbers for switches, or IP addresses/netmasks for VPN servers

RADIUS Online Resources

- freeradius.org is the website with software, case studies, documentation, support wiki, and links to additional resources
- wiki.freeradius.org/guide/HOWTO has examples of setting up various access scenarios
- linuxexplore.com/how-tos/pam-with-radius-authentication/ has simple instructions to enable PAM to use RADIUS
- A full technical guide for FreeRADIUS including protocol discussions is available at networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf



Authentication Lab

- RADIUS service install
- pam_radius setup with sshd