Linux Academy: SSH and Secure Access – Course Notes
http://linuxacademy.com

Video One – SSH and ~/.ssh/knownhosts

- ssh
  - secure shell client for accessing Linux/Unix servers
  - replaced the much less secure (read: everything was transmitted over plain text) 'telnet' method of accessing systems
  - options
    - -l: login as (username)
    - -v: verbose
      - will provide additional information during login (encryption type, system response, ssh server version)
      - used during troubleshooting ssh connections
    - -vv: very verbos
    - -vvv: ridiculously verbose
  - installation of server
    - RPM: 'sudo yum install openssh-server'
    - Debian: 'sudo apt-get install openssh-server'
  - default RSA encryption
  - create 'knownhosts' file to track ip and and mac address pairing for future verification of system connections
- knownhosts
  - hash key created, using the mac address of the connecting system's IP and mac adress to build
  - rebuilding server will invalidate the hash for the server even if name is the same
  - not usable by other systems since no identifying information is hashed unencrypted

Video Two – ssh-keygen

- ssh-keygen
  - generates public and private keypairs in a variety of encryption methods (RSA and DSA are the current primary encryption types) for exchanging between systems in order to use for passwordless but secure login
  - options
    - -t rsa: generate an encryption keypair using the (default) and more secure RSA encryption method (both public and private keys are generated)
    - -t dsa: generate an encryption keypair using the legacy DSA encryption method (both public and private keys are generated)
    - -i <file>: read (un)encrypted input keyfile to use for generating public key
    - -f <file>: name the output file as indicated
  - ssh equivalent to the public and private keys that are used in SSL certificates
  - when used in conjunction with the SYSTEM generated keyfiles (see Video Three), completes a security chain that secures the connection locally, remotely and in transit

Video Three – ssh key types and ssh-copy-id

- key types
  - RSA: most widely used encrytion method, used with SSH1 and SSH2, 2048 bit in size
  - DSA: included with SSH2, complex algorithm for decoding which can slow down transactions, although 2048 bit is allowed, 1024 bit is default size
- ssh-copy-id
  - allows copy of public key to remote authorized key file
  - authorized_keys

    - hashed key list pair of hosts and public keys that are allowed to connect without password to the host, although passphrases are still required (passphrases will be required even if the remote host is running ssh-agent, but it will be invisible to server and client)
    - example:
      - ssh-copy-id user@remote-server-ip
      - -i <file>: use the indicated key file rather than the default RSA key

Video Four – ssh-agent and ssh-add

- ssh-agent
  - program used to hold private keys for public key exchange (RSA or DSA)
  - designed to run on already started X windows or shell environments for caching of key exchange and identity management
    - options:
      - -a <address>: bind to indicated address
      - -k: kill running agent
      - -t <file>: include indicated identity rather than default keys
- ssh-add
  - program for adding private key identities to running ssh-agent
  - options:
    - -d/D <identity>: delete indicated or all identities from running agent
    - -l/L: list properties of all identities currently installed (can be used to get identity to delete)
    - -t <time>: time to live for identity, in seconds, to be loaded into agent
    - -x: lock agent with a password
    - -X: unlock the agent

Video Five – System RSA/DSA Key Types

- system RSA key
  - pub and key file
    - RSA key for the system, generated on installation and initial start of open-ssh server
    - used much the same as certificate keys are for SSL certificates
      - a secure SSH chain contains:
        - server side: imported public key from trusted client, system public and private keys
        - client side: received public key from server, client public and private keys
- system DSA key
  - pub and key file
    - DSA key for the system, generated on installation and initial start of open-ssh server
    - used much the same as certificate keys are for SSL certificates
      - a secure SSH chain contains:
        - server side: imported public key from trusted client, system public and private keys
        - client side: received public key from server, client public and private keys

Video Six – PGP and GnomePG/.gnupgp

- PGP
  - “pretty good protection” - a method of encrypting and verifying personal online transactions using standard protocol and practice
  - implemented for emails, online purchases, personal transactions, hard drive and external drive encryptions, etc
- GnomePG/.gnupg
  - gnome specific encryption, keys can be generated and appended to email or other transactions to authenticate the origin of the transaction
    - GnuPG is the suite of encryption programs
    - key generation:

  - gpg –gen-key
    - following prompts to generate the key (RSA is default), size of key (1024/2048), expiration, etc
    - passphrase will then begin to generate the key (can take a few minutes)
  - pub and key files with a signature file are generated
  - gpg –export-secret-keys > keyfile.asc
    - backing up the key files
- can be exported to a key server
  - gpg –keyserver hkp://local.key.srv –send-key KEYNAME
    - KEYNAME: key ID of your primary keypair as saved during generation
- can be revoked
  - gpg –output REVOKE.FILE –gen-revoke KEYNAME
    - without the output option, all output will go to standard output (console) and there could be a lot, so a file will make it easier to review after