

# Security

## CIS 68C2 UNIX Network Administration

Updated: 12/4/02

CIS68C2 UNIX Network Administration  
Copyright 2002 - Mike Cappella

1

# Security

- Types of Network Threats
  - ✗ Unauthorized Access
  - ✗ Information Disclosure
  - ✗ Denial of Service

Updated: 12/4/02

CIS68C2 UNIX Network Administration  
Copyright 2002 - Mike Cappella

2

# Security

- Prevention
  - ✗ Common sense administrative approach and philosophy
    - ✗ Ensure built-in security mechanisms are used appropriately
    - ✗ Adopt a Disable Until Needed philosophy
  - ✗ Remove or disable unnecessary software and services
  - ✗ Track security sites and news
    - ✗ Vendor, newsgroups, FIRST, NIST, CERT advisories, SANS Institute, Exploit sites

Updated: 12/4/02

CIS68C2 UNIX Network Administration  
Copyright 2002 - Mike Cappella

3

# Security

- Prevention
  - ✗ Apply security patches promptly and routinely
  - ✗ Proactively learn about inherently insecure services
    - ✗ CGI, r commands, ftp, telnet
  - ✗ Replace insecure services with secure alternatives

Updated: 12/4/02

CIS68C2 UNIX Network Administration  
Copyright 2002 - Mike Cappella

4

# Security

- Detection
  - ✗ Learn what “feels” normal to help detect anomalies
  - ✗ Monitor system logs daily
  - ✗ Use analysis tools such as logwatch and tripwire
  - ✗ Scan the system for known exploits

# Security

- SSH – Secure Shell
  - ✗ Securely Replaces the r Commands
    - ✗ **Authentication** ensures trusted host really is the trusted host
    - ✗ **Encryption** ensures data is encrypted to prevent eavesdropping
  - ✗ Two versions of SSH
    - ✗ **SSH Secure Shell** – Commercial product
    - ✗ **OpenSSH** – Open Source product
  - ✗ Two SSH protocol versions: **SSH1** and **SSH2**
    - ✗ SSH1 is considered very insecure – use SSH2 whenever possible

# Security

- SSH Components
  - ✗ **sshd**
    - ✗ Server-side daemon that handles incoming SSH connections
  - ✗ **ssh**
    - ✗ Client-side SSH user command
    - ✗ Securely logs in or passes command to remote system
  - ✗ **ssh-keygen**
    - ✗ Generates public / private RSA or DSA keys
  - ✗ **sftp / scp**
    - ✗ Secure versions of ftp / rcp

# Security

- DSA
  - ✗ Digital Signature Algorithm
  - ✗ Published by NIST
    - ✗ National Institute of Standards and Technology
  - ✗ Provides secure authentication, not encryption
- RSA
  - ✗ Encryption and authentication system
    - ✗ Developed by **R**ivest, **S**hamir and **A**dleman
    - ✗ Owned and licensed by RSA Security
  - ✗ Used by many applications and protocols
    - ✗ Browsers, SSH, Lotus Notes, Quicken
    - ✗ S/MIME, S/WAN, SSL

# Security

- RSA
  - ✗ Encryption
    - ✗ Two large prime numbers are used to generate two other numbers called the **public key** and the **private key**
      - ✗ Both keys are required
      - ✗ Public key is shared and used by others
      - ✗ Private key is secret
        - ✗ Only known by user, never set over network
      - ✗ Private and public key reverse actions of each other
        - ✗ Public key decrypts private key encrypted messages, and vice versa
  - ✗ Authentication
    - ✗ Established and ensured by exchanging an encrypted **digital certificate** with each message

# Security

- Diffie-Hellman
  - ✗ Used to securely exchange data encrypt keys over an insecure network
  - ✗ Creates a **shared secret** used to encrypt symmetric keys

# Security

- SSH Connection Overview
  - ✗ Client contacts server
  - ✗ Connection is secured at the Transport Layer
  - ✗ Communication over the connection is encrypted
  - ✗ Client authenticates itself with server
    - ✗ Authentication data is encrypted since transport layer is encrypted
  - ✗ Remote login is established, or remote command runs
  - ✗ Other services can be tunneled through the connection
    - ✗ **Port forwarding**

# Security

- SSH - Establishing a secure Transport Layer
  - ✗ Client and server exchange public keys
  - ✗ Client and server negotiate and agree on choice of :
    - ✗ **Public key** algorithm
      - ✗ RSA, DSA
    - ✗ **Cyphers** - symmetric encryption (shared secret) algorithms
      - ✗ DES, 3DES, 128/192/256-bit AES, Blowfish, CAST128, Arcfour
    - ✗ **Message authentication** (hash, data integrity) algorithm
      - ✗ hmac-md5[-96], hmac-sha1[-96], hmac-ripemd160
  - ✗ Randomly generated **session key** created from public key
    - ✗ Session key (shared secret) is used to encrypt communication for the duration of the SSH connection

## Security

- SSH – Authentication methods
  - ✗ RhostsAuthentication
    - ✗ ~/.rhosts, ~/.shosts, /etc/hosts.equiv, /etc/shosts.equiv
    - ✗ Not very secure – not recommended
  - ✗ RhostsRSAAuthentication
    - ✗ RhostsAuthentication but also requires RSA authentication
    - ✗ Still not very secure – not recommended
  - ✗ RSAAuthentication
    - ✗ Per-user RSA public key authentication
    - ✗ Requires private key file locally, and password to decrypt it
  - ✗ PasswordAuthentication
    - ✗ Normal login passwords

## Security

- SSH - Global Configuration Files
  - ✗ Red Hat: files live under /etc/ssh

File	Used by	Description
ssh_config	ssh	Master client config file overridden by user's ~/.ssh/config
sshd_config	sshd	Master server configuration file
ssh_host_dsa_key	sshd	DSA private key
ssh_host_dsa_key.pub	sshd	DSA public key
ssh_host_key	sshd	RSA private key for SSH v1
ssh_host_key.pub	sshd	RSA public key for SSH v1
ssh_host_rsa_key	sshd	RSA private key for SSH v2
ssh_host_rsa_key.pub	sshd	RSA public key for SSH v2
moduli		Diffie-Hellman groups used for Diffie-Hellman key exchange

## Security

- SSH - User Configuration Files
  - ✗ Red Hat: files live under ~/.ssh

File	Private	Description
authorized_keys		List of authorized public keys
id_dsa	yes	User's DSA authentication identity
id_dsa.pub		User's DSA public key
id_rsa	yes	User's RSA public key for SSH v2
identity		User's RSA private key for SSH v1
known_hosts		List of DSA host keys of the SSH servers user has accessed

## Security

- SSH – Port Forwarding
  - ✗ SSH can securely forward TCP/IP ports
  - ✗ Traffic to remote server passes through the secure SSH channel
  - ✗ Provides secure connections to other services
  - ✗ Local service is configured to connect to localhost
    - ✗ ssh creates socket to listen for incoming connections
  - ✗ Remote sshd sends forward packets to destination service

## Additional Information

- Recommended SSH and Security-related Sites
  - × OpenSSH
    - × <http://www.openssh.com/>
  - × SSH Communications Security
    - × <http://www.ssh.com/>
  - × Red Hat SSH Overview
    - × <http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/ref-guide/ch-ssh.html>
  - × RSA Security
    - × <http://www.rsasecurity.com/>