SSH -- Secure Shell

Discussion Notes
rev4
Cyber Security Forum
nebraskacert.org/CSF/
Some SSH Hardening

- Many SSH installations have dangerous default settings enabled.
- This talk discusses some of these vulnerabilities, how to check for them, and ways to mitigate them.
- Additionally, some good practices (and handy tricks!) for using SSH to improve security are proposed and demonstrated.
Why does this happen?

• Just as older httpd installations have default settings that are now considered bad practices, many sshd installations have default settings that present vulnerable attack surfaces.

• TAM, features, and easy of use
About

• Speaker:
  – Matt Payne, CISSP
  – Contact: Payne@MattPayne.org or (402) 208-8787

• Slides:
  – Available online at http://MattPayne.org/ssh
  – RSS Feed for updates:
    • http://www.mattpayne.org/blog/category/programming/ia/ssh/feed
  – License
    • http://creativecommons.org/licenses/by-sa/2.5/
Outcomes & Agenda

- SSH knowledge you can put to work that same day:
  - (0) SSH Basics
  - (1) Does your network allow SSH tunneling to violate your firewall policy? web content filtering policy? VPN policy?
  - (2) Use SSH to create two factor authentication and improve logging
  - (3) Use OpenSSH configuration options to narrow the use of SSH’s features to specific use cases
  - (4) Lower the risk of MiTM attacks. (5) Use SSH as network duct tape.
SSH Basics

• SSH provides:
  – Terminal services (putty, ssh, etc)
  – Remote command execution
    • ssh server “tar -czpf -” | tar xzpf -
      – http://tinyurl.com/yztu4m
  – File transfer services (scp, sftp)
    • Emacs tramp builds on this & linux has a fuse.sf.net based ssh filesystem…
  – Port forwarding -- aka tunneling
    • Local (TCP listens on local box) connects to remote
    • Remote (TCP listens on remote box) connects to local
    • Dynamic (TCP listens on local box) connects to changing remote endpoints acting as a SOCKS proxy…
    • There are many handouts on using VNC and SSH tunnels…..
X11 (X.org) windows forwarding

- Want to run a X gui remotely (SMIT on AIX whatever)…
- `ssh -X user@otherbox`
- Now `$DISPLAY` is not :0.0 it’s :0:10 and running xeyes (or other gui) opens on the computer that ran ssh -X
- May have to run xauth (YMMV)
Handy Authentication!

• Password Based authentication
• Key pair (public key, private key)
  – SSH access is granted to any account where the public key is in authorized_keys and the ssh client has access to the corresponding private key.
  – Private keys may have pass phrases
    • Two factor authentication!
    • We’ll see how to avoid carpal tunnel with ssh-agent
• It’s possible to connect to many different authentication mechanisms -- single signon can be done… Should it?
Handy Uses

• Beyond terminals and file transfers there is….
  – Using X Windows (X11, kde, gnome) across the network
  – Adding encryption to network services: POP, SMTP, CVS, SVN, NFS, samba, printing, rsync, etc

• Recall that the xinetd/inetd model is for the network service to read from stdin & write to stdout then xinetd/inetd does the TCP stuff…
Remote Commands

• ssh user@server “ls -lt”
  – # What’s in the $HOME directory?
• ssh user@server “cat /etc/passwd” | grep -l steve | tee steves.txt | wc -l
• Accounting? Does remote command execution show up via the output of “last”?  
  TODO: Where is it logged by default in the ubuntu being used this semester?
SSH Litmus Testing

• Does your network allow SSH tunneling to violate your firewall policy?
• Web content filtering policy?
• VPN policy?
  – Try it with putty!
  – But remember Randal Schwartz first!
• Example: Suppose your network only allows outbound port 25 (SMTP) connections to mail.corporate.com
Local Tunnels

- Can renumber ports -- connect localhost:80 to somebox.com:8080
- Suppose an ISP does not allow you to connect to anyone’s port 25 but their SMTP’s server’s port 25….
- “The internet treats censorship as a defect and routes around it.” -- John Gilmore
- ssh user@somebox.com -L 25:localhost:25
  - Now email clients (MUAs) may connect to localhost’s port 25 which is not prevented by the ISP router ACLs.
  - The ssh client accepts the port 25 connection, forwards the data to the ssh server (sshd; d is for daemon) where a connection is made to localhost:25 to forward the data.
    - Sshd’s localhost is somebox.com -- outside of the ISP’s router’s ACLs’ control.
sudo ssh -L 25:127.0.0.1:25 account@somebox.com

• On windows with putty this looks like:
  • -L is for local
  • The TCP listen is done on the local box
    – Where the client runs
Remote Tunnels

• A database application connects to mySQL on localhost:3306. You want to move the mySQL server off the application box without changing the application…

• Database server boxes connect to provide the service:
  – ssh user@applicationbox -R 3306:localhost:3306
    • Many database servers can take turns providing the service…
Collaborating...

• You’re asked to help people on a UNIX box behind a NAT. They can ssh to the Internet but boxes on the Internet cannot login to the box behind the NAT...

• Ask your customer to:
  – ssh guestuser@some.internetbox.com -R 2000:localhost:22
  – kibitz youraccount  # part of expect.nist.gov
  – ssh localhost -p 2000 -l customerlogin
Dynamic Port Forwarding…

- Web browsers and other programs (e.g. some IM clients) are SOCKS aware.
- `ssh -D 9090 user@server.com`
- Now localhost:9090 acts as a SOCKS proxy.
  - Browser (once configured) connects to localhost:9090
  - Request is passed encrypted via port 22 to sshd
  - sshd makes connection (e.g. to TheOnion.com)
- Older articles will talk about local tunnels to Squid-cache.org proxies. This works too….
Dynamic Port Forwarding with Putty

• First start putty with a dynamic tunnel
• Second configure your web browser to be a SOCKS client
• Third surf with:
  – “privacy”
  – Access to your Intranet
  • DNS lookups happen on the box running ssh server (sshd)
Putty Dynamic Tunnels
IE as a SOCKS client

- IE Tools Menu
  - Internet Options
    - Connections Tab
      - LAN Settings Button
        » Advanced Button
Local and Remote
When the tunnel is gone..
Meet in the middle tunnels

- U$ ssh -R2222:127.0.0.1:22 payne@R
- M $ ssh 192.168.0.3 -L 22:localhost:2222
- Privileged ports can only be forwarded by root.
- M $ sudo ssh 192.168.0.3 -L 22:localhost:2222
- Password:
- root@192.168.0.3's password:
- M $ sudo ssh payne@192.168.0.3 -L 22:localhost:2222
- payne@192.168.0.3's password:
- Last login: Wed Nov 29 01:49:18 2006 from 192.168.0.4
- [payne@R ~]$  

- M$ ssh localhost
- Linux payne 2.6.15-23-386 #1 PREEMPT Tue May 23 13:49:40 UTC 2006 i686 GNU/Linux
- U$  
- REFERENCE: portforward.com
SSH for Two Factor Authentication
## PK auth -- 1st Time

<table>
<thead>
<tr>
<th>Step</th>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>ssh-keygen -t rsa</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Copy <code>~/.ssh/id_rsa.pub</code> to <code>server:/tmp</code></td>
<td>Append <code>/tmp/id_rsa.pub</code> to <code>~/.ssh/authorized_keys</code> on server. &lt;br&gt;chmod 600 <code>authorized_keys</code> on server.</td>
</tr>
<tr>
<td>3</td>
<td><code>ssh server</code></td>
<td>You’re connected after entering private key’s passphrase (which may be blank)</td>
</tr>
</tbody>
</table>
PK & Password Auth

• Both public key and password authentication may be active!
• Changing account’s password does not invalidate the keys in ~/.ssh/authorized_keys
SSH for Improved Logging
authorized_keys eg:

- Examples (from man 8 sshd)
  1. `1024 33 12121...312314325 ylo@foo.bar`
  2. `from="*.niksula.hut.fi,!pc.niksula.hut.fi" 1024 35 23...2334 ylo@niksula`
  3. `command="dump /home",no-pty,no-port-forwarding 1024 33 23...2323 backup.hut.fi`
  4. `permitopen="10.2.1.55:80",permitopen="10.2.1.56:25" 1024 33 23...2323`
Example authorized_keys

- permitopen="ca.ist.unomaha.edu:22" ssh-rsa
  AAAAB3NzaC1yc2EAAAABIwAAAQEAyltw4JJQcGr+xReTnpELRuD9SHpNHK3E AoMUoO+GFgWgwHli3QewGCaVlvjGq04bGuVPiHxbD/8c83TNWqPQ5ehfj0aw2L5b05/E UdHzVd9DKWxelZB6psmblefqmJ6AGv+AuzWxhyUYoMGg8GTIVAmKOXAIZ+XL2Y/oefjsesL9d5fl+rJoT5YCDpVG81EDP5HiMMkVqaAium+cfgwl3sFMdvlvZxuNdBZeC8FY32q98UwfeUXfxDI9z6xOjaJC5hd2tw70j0x3HJdRFbQEPJdnZZfT/0GvMcOgh5D54SQiaFE2FCwPDN0qFMqGO79jg4cZ6MPDyqvFQ256UpGcbw== payne@matt-paynes-computer.local
Using find...

- No surprise authorized_keys files
- Wouldn’t it be nice if PKs had expiration dates!
- Script to coordinate last (and other logs) and authorized_keys files
  - User goes inactive for X days and their public keys are set to only execute a cat /etc/contact-security command....
Narrowing SSH use cases
Lower the risk of MiTM Attacks
SSH as Network Duct Tape
SSH Basics
Limiting & commenting PKs

• http://tinyurl.com/yddkk5 says:
  • Each line of authorized_keys contains up to three items in order, some optional and some required:
    – A set of options (optional, surprise, surprise).
    – The public key (required).
    – A descriptive comment (optional). This can be any text, such as "Bob's public key"
    – Comments may also start with #

• Options include (cf “man 8 sshd”):
  – permitopen
  – command
  – from
  – environment
  – no-port-forwarding
ssh-agent: avoiding carpel tunnel…

- **OS X**: sshkeychain.org
  - matt-paynes-computer:~ payne$ env | grep SSH
  - SSH_AUTH_SOCK=/tmp/501/SSHKeychain.socket
  - matt-paynes-computer:~ payne$

- **Ubuntu & other unix**: ssh-agent
  - ssh-agent bash  # Start a bash w/ env vars
  - ssh-add # Add identity to agent…
Example....

- `payne@payne:~$ ls .ssh`
- `authorized_keys id_rsa id_rsa.pub known_hosts`
- `payne@payne:~$ cat .ssh/id_rsa.pub |ssh ca.ist.UNOmaha.edu 'cat >> .ssh/authorized_keys'`
- `payne@ca.ist.unomaha.edu's password:`
- `payne@payne:~$ ssh ca.ist.UNOmaha.edu`
- `Enter passphrase for key '/home/payne/.ssh/id_rsa':`
- `Last login: Wed Nov 29 14:14:08 2006 from rp614v3.ist.unomaha.edu`
- `[payne@cist4370 ~]$`
Example cont....

- `payne@payne:~$ ps`
- `PID TTY          TIME   CMD`
- `3036 pts/3  00:00:00 bash`
- `3060 pts/3  00:00:00 ps`
- `payne@payne:~$ ssh-agent bash`
- `payne@payne:~$ ps`
- `PID TTY          TIME   CMD`
- `3036 pts/3  00:00:00 bash`
- `3063 pts/3  00:00:00 bash`
- `3083 pts/3  00:00:00 ps`
- `payne@payne:~$ ssh-add`
- `Enter passphrase for /home/payne/.ssh/id_rsa:`
- `Identity added: /home/payne/.ssh/id_rsa (/home/payne/.ssh/id_rsa)`
- `payne@payne:~$ ssh ca.ist.UNOmaha.edu`
- `[payne@cist4370 ~]$`
Avoiding MITM attacks

- Most PK schemes (SSH, SSL, PGP, etc) are open to Man in the Middle Attacks
  - http://tinyurl.com/pbkd9
- A known_hosts file can be kept at the machine level and the account level
- Holds key ids for sshds connected to
Tweaking OpenSSH configs

- `sshd_config` (typically in `/etc/ssh`)
  - Out of the box: `PermitRootLogin yes`
    - Should be no! Why?
  - Out of the box: Tunneling is on! man `sshd_config` says:
    - `AllowTcpForwarding`
      - Specifies whether TCP forwarding is permitted. The default is ``yes``. Note that disabling TCP forwarding does not improve security unless users are also denied shell access, as they can always install their own forwarders.
      - Should `AllowTcpForwarding` and `X11Forwarding` really be on out of the box? There is a way to permit only certain users to tunnel...
Permitting only one tunnel

• `root@payne:/home/payne/.ssh#`
  – `chown root.root authorized_keys`
• `root@payne:/home/payne/.ssh#`
  – `chmod a+r authorized_keys`
• `root@payne:/home/payne/.ssh#`
  – `grep permit authorized_keys`
• `permitopen="ca.ist.unomaha.edu:22" ssh-rsa AAAAB3NzaC1yc2EAAAABImwAAAQEAyltw4J JQcGr+ **Truncated**`
But, password
PasswordAuthentication no??

• Needed to limit tunnels to special users….
• Will users put up with this?
• http://www.gentoo.org/proj/en/keychain/
• Pagent.exe — SSH key agent
  http://tinyurl.com/gpj8c
• OS X sshkeychain.org
Turning off tunnels at the client

- In /etc/ssh_config set to no
  - DynamicForward
  - LocalForward
  - RemoteForward
- Putty and other clients?
- Microsoft’s Port Reporter?
Auth.log out of the box

• Nov 29 10:46:27 payne sshd[3458]: Accepted publickey for payne from 127.0.0.1 port 44503 ssh2
• Nov 29 10:46:27 payne sshd[3460]: (pam_unix) session opened for user payne by (uid=0)
• Tweak:
  – root@payne:/etc/ssh# grep LogLevel sshd_config
  – #LogLevel INFO
  – LogLevel VERBOSE
  – root@payne:/etc/ssh# /etc/init.d/ssh restart
  – * Restarting OpenBSD Secure Shell server...
  – ...done.
  – root@payne:/etc/ssh#
Auth.log after tweak

- Nov 29 10:48:34 payne sshd[3549]: Failed none for payne from 127.0.0.1 port 44504 ssh2
- Nov 29 10:48:34 payne sshd[3549]: Found matching RSA key:
- Nov 29 10:48:34 payne sshd[3549]: Found matching RSA key:
- Nov 29 10:48:34 payne sshd[3549]: Accepted publickey for payne from 127.0.0.1 port 44504 ssh2
- Nov 29 10:48:34 payne sshd[3553]: (pam_unix) session opened for user payne by (uid=0)
Matching auth.log to authorized_keys

- `payne@payne:~$ while read pubkey
-   > do
-   >   echo $pubkey > /tmp/pk
-   >   ssh-keygen -l -f /tmp/pk
-   >   done < .ssh/authorized_keys
- `payne@payne:~$
- Thanks google and http://tinyurl.com/yh2875
Mantra: Implementation & Key Management

- Implementation story
  - Buffer Overflow
    - P.156 of ORA.com’s Network Security Assessment by Chris McNab
    - Using NVD.gov to track software versions…
  - Mantissa attack

- Key Management story:
  - Mystery lab scenario from 11/21/2006
  - Mitigation -- crontab that deletes authorized_keys if no login within X days? Or crontab that makes security administrators aware…
Check these out…

• “Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints”

• Refs
  – rSync and SSH
    • http://www.linuxtoday.com/storage/2006082100526OSHLSV
  – GDB and SSH Tunneling
    • http://www.cucy.net/lacp/archives/000024.html
    – http://souptonuts.sourceforge.net/sshtips.htm
    – http://proxytunnel.sourceforge.net/users.php
Squid for Privacy

- COTSE.net
  - Church of the Swimming Elephant
    - Proxies and more for $6/month

- Many people just setup Squid, connect to it with a SSH tunnel and stop there…
  - squid-cache.org

- Or use a dynamic tunnel….
2006 Articles on SSH

- Tunnelling with SSH -- Oct 2006

- Mitigating the Security Risks of SSH -- Aug 2006


- SSH Tunnels: Bypass (Almost) Any Firewall --- Aug 2006
Misc Refs

• Libraries

• MAC?
Questions?

• **Speaker:**
  - Matt Payne, CISSP
  - Contact: Payne@MattPayne.org or (402) 208-8787

• **Slides:**
  - Available online at http://MattPayne.org/ssh
  - RSS Feed for updates:
    • http://www.mattpayne.org/blog/category/programming/ia/ssh/feed
  - License
    • http://creativecommons.org/licenses/by-sa/2.5/