(Mis)trusting and (ab)using ssh

- 1.

  (mis)Trusting and (ab)UsingSSH Tips and Tricks for Pentesters and Sysadmins Herman Duarte <hcoduarte@gmail.com> Bruno Morisson <morisson@genhex.org> Monday, July 2, 12 1

- 2.

  About us Bruno Morisson Herman Duarte <morisson@genhex.org> <hcoduarte@gmail.com> http://genhex.org/~mori/ I do security stuff @ INTEGRITY S.A. InfoSEC addict @ INTEGRITY S.A. @morisson @hdontwit http://www.linkedin.com/in/morisson http://www.linkedin.com/in/hcoduarte Monday, July 2, 12 2

- 3.

  In the beginningof times... Telnet r* services (rlogin, rsh) Weak (or no) authentication Communication in clear Monday, July 2, 12 3

- 4.

  In the beginningof times... Sniffing Interception Hijacking Man-In-The-Middle ... Monday, July 2, 12 4

- 5.
- 6.

  SSH* features Key agreement (DH) Encrypted communications (C&I from CIA) Multiple authentication options (password, public keys, kerberos, etc...) Channel Multiplexing Port Forwarding VPN ...and so much more! * for this talk SSH==SSHv2 Monday, July 2, 12 6

- 7.
- 8.

  SSH 101- TheBasics Session Multiplexing, TCP forwarding, Connection socket forwarding, sftp subsystem, etc SSH User Auth User Authentication (password, Pubkey, etc) Key Agreement (DH), Host auth, Integrity, Transport Encryption, Re-Keying TCP IP Monday, July 2, 12 8

- 9.

  SSH 101- TheBasics Encrypted Channel Setup User Authentication Client Connection Server Monday, July 2, 12 9

- 10.

SSH 101- TheBasics User authentication methods: GSSAPI Host-Based Public Key Challenge-Response Password Monday, July 2, 12 10

- 11.

Password Authentication Encrypted Channel Setup Client Server username, use password OK Password Auth Ok / NOk passwd ssh sshd file Monday, July 2, 12 11

- 12.

If the serveris compromised... sshd binary is changed with one that logs passwords keylogger is installed on the server ..the password is compromised! Monday, July 2, 12 12

- 13.

PublicKey Authentication Encrypted Channel Setup Client Server username, use publickey OK Signature Auth Ok / NOk authorized id_dsa ssh sshd _keys Monday, July 2, 12 13

- 14.
- 15.

What if Ihave a lot of keys, or login a lot ?? Monday, July 2, 12 15

- 16.

SSH Agent Encrypted Channel Setup Client Server username, use publickey OK Signature Auth Ok / NOk Agent ssh sshd authorized id_dsa _keys Monday, July 2, 12 16

- 17.

What if ISSH into other servers ?? Monday, July 2, 12 17

- 18.

SSH Agent Forwarding No need to copy private key to other servers Key is kept on the original source host Agent is forwarded, using a tunnel Passwordless! Monday, July 2, 12 18

- 19.

SSH Agent Forwarding Client Transport Server #1 Transport Server #2 Connection Connection Interactive Shell Agent Forwarding Interactive Shell Agent ssh sshd ssh sshd authorized authorized id_dsa _keys _keys Monday, July 2, 12 19

- 20.

Control Master Connection multiplexing allows for multiple sessions on one connection It’s fast No need for extra authentication Monday, July 2, 12 20

- 21.

- 22.

  Caveat Emptor(s) You must trust the server(s) What if the server was compromised ? Can SSH Agent be abused ? Can Control Master be abused ? Monday, July 2, 12 22

- 23.
- 24.

  Help us ObiWan You're our only hope! Monday, July 2, 12 24

- 25.

  Freak on aLeash When adding keys to ssh-agent use ssh-add with: -t <secs> to set a maximum lifetime on the identities being added to the agent -c to indicate that identities being added should be subject to confirmation before being used for auth Monday, July 2, 12 25

- 26.

  Freak on aLeash ssh-agent queries /usr/libexec/ssh-askpass for confirmation "ssh-add -c -t 3600 < /dev/null" makes ssh-add use env var SSH_ASKPASS to query for passphrase Monday, July 2, 12 26

- 27.
- 28.

  But we stillneed passwords! If you su / sudo, you still type your password... What if we could use the SSH Agent for sudo ? Yes we can! :) Monday, July 2, 12 28

- 29.
- 30.
- 31.
- 32.

  Using SSH w/ousing SSH (but still using SSH) ssh -W trusted:22 untrusted Open socket to trusted Server... ...through an untrusted Server Monday, July 2, 12 32

- 33.

  Using SSH w/ousing SSH (but still using SSH) Connect to the socket created ssh -o "ProxyCommand ssh -a -W trusted:22 untrusted" trusted Disable Agent Forwarding Open Socket to trusted via untrusted Just for user and key validation Monday, July 2, 12 33

- 34.

  Using SSH w/ousing SSH (but still using SSH) Client Transport Untrusted Owned Trusted Connection -W (Open Socket to Server #2) Transport Connection Interactive Shell Agent ssh sshd sshd authorized authorized id_dsa _keys _keys Monday, July 2, 12 34

- 35.

- 36.

  Control your SSH .ssh/config Host trusted1 trusted2 trusted3 ForwardAgent yes ProxyCommand ssh -a -W %h:22 untrusted.server.com Host * ControlMaster no ForwardAgent no PasswordAuthentication no HashKnownHosts yes Monday, July 2, 12 36

- 37.
- 38.

  References RTFM :) RFCs 4251-4256,4335,4344,4345,4419,4432,4462,4716,56 56 http://www.linuxjournal.com/article/9566 http://pamsshagentauth.sourceforge.net/ http://www.jedi.be/blog/2010/08/27/ssh-tricks-the- usual-and-beyond/ Monday, July 2, 12 38
