

understanding chkrootkit: sshd section

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2001-12/0844.html>

From: gaius.petronius (rut@linuxmail.org)

Date: 12/30/01

From: rut@linuxmail.org (gaius.petronius)

Date: 30 Dec 2001 00:23:43 -0800

installed chkrootkit 0.34 on a Mandrake 8.1 Linux kernel 2.4n system connected to an internal network.

i wanted to see what kind of activity it would report since i am very confident that this machine is clean.

lo and behold running this inept mode './chkrootkit -x' yields a load of crap that i have no [expletive deleted] idea what the [expletive deleted] it means, like:

Output of: /usr/bin/strings -a /bin/ps

###

```
/lib/ld-linux.so.2
__gmon_start__
libproc.so.2.0.7
dev_to_tty
procps_version
Hertz
_DYNAMIC
ps_readproc
reset_sort_options
read_total_main
open_psd
_init
display_version
openproc
look_up_our_self
linux_version_code
closeproc
uptime
_fini
wchan
_GLOBAL_OFFSET_TABLE_
libc.so.6
```

nevertheless, in the hope that this endless stream of incoherency would at last come to life i plowed through this crap and stumbled

onto this: a section on sshd.

i snipped only what seems to belong to the sshd section.

i am inclined to believe that it tells me only one thing: that the machine used to have another name and that the .ssh/known_hosts key must be deleted for the old name.

other than that i see no coherent message from this bundle of programs.

can anyone help me read the output of 'chkrootkit -x' and help me guess what this [expletive deleted] piece of [expletive deleted] is trying the [expletive deleted] to say?

and TIA to all.

chkroot crap snippet here:

SSH PRIVATE KEY FILE FORMAT 1.1

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-

@(#)\$OpenBSD: ssh.c,v 1.116 2001/04/17 12:55:04 markus Exp \$

Usage: %s [options] host [command]

- l user Log in using this user name.
- n Redirect input from /dev/null.
- A Enable authentication agent forwarding.
- a Disable authentication agent forwarding.
- X Enable X11 connection forwarding.
- x Disable X11 connection forwarding.
- i file Identity for public key authentication (default: ~/.ssh/identity)
- t Tty; allocate a tty even if command is given.
- T Do not allocate a tty.
- v Verbose; display verbose debugging messages.
Multiple -v increases verbosity.
- V Display version number only.
- P Don't allocate a privileged port.
- q Quiet; don't display any warning messages.
- f Fork into background after authentication.
- e char Set escape character; ``none" = disable (default: ~).
- c cipher Select encryption algorithm: ``3des", ``blowfish"
- m macs Specify MAC algorithms for protocol version 2.
- p port Connect to this port. Server must be on the same port.
- L listen-port:host:port Forward local port to remote address
- R listen-port:host:port Forward remote port to local address
These cause %s to listen for connections on a port, and forward them to the other side by connecting to host:port.
- C Enable compression.
- N Do not execute a shell or command.

-g Allow remote hosts to connect to forwarded ports.
-1 Force protocol version 1.
-2 Force protocol version 2.
-o 'option' Process the option as if it was read from a configuration file.
-s Invoke command (mandatory) as SSH2 subsystem.
Using rsh. WARNING: Connection will not be encrypted.
Warning: Identity file %s does not exist.
Too many identity files specified (max %d)
%s, SSH protocols %d.%d/%d.%d, OpenSSL 0x%8.8lx
Bad forwarding specification '%s'.
You must specify a subsystem to invoke.
Cannot fork into background without a command to execute.
Pseudo-terminal will not be allocated because stdin is not a terminal.
Rhosts Authentication disabled, originating port will not be trusted.
Could not create directory '%.200s'.
; reverting to insecure method
Secure connection to %.100s on port %hu refused%.100s.
Secure connection to %.100s refused%.100s.
%.100s list %.200s 2>/dev/null
Connections to local port %d forwarded to remote address %.200s:%d
Could not request local forwarding.
Connections to remote port %d forwarded to local address %.200s:%d
Requesting compression at level %d.
Compression level must be from 1 (fast) to 9 (slow, best).
Warning: Remote host refused compression.
Protocol error waiting for compression response.
Warning: Remote host failed or refused to allocate a pseudo tty.
Protocol error waiting for pty request response.
Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding.
Protocol error waiting for X11 forwarding
Requesting authentication agent forwarding.
Packet integrity error (%d != %d) at %s:%d
Warning: Remote host denied authentication agent forwarding.
Packet integrity error (%d bytes remaining) at %s:%d
Request for subsystem '%.*s' failed on channel %d
Options:
-4 Use IPv4 only.
-6 Use IPv6 only.
/usr/bin/rsh
setrlimit failed: %.100s
You don't exist, go away!
eilcmpLRDo
Too high debugging level.
OpenSSH_2.9p2
none
Bad escape character '%s'.
Unknown cipher type '%s'
3des-cbc
blowfish-cbc

Unknown mac type '%s'
Bad port '%s'
%hu/%255[^/]/%hu
%hu:%255[^:]:%hu
Bad dynamic port '%s'
command-line
.ssh/config
%.100s/%.100s
/etc/ssh/ssh_config
rsh_connect returned
/etc/ssh/ssh_host_key
/etc/ssh/ssh_host_dsa_key
/etc/ssh/ssh_host_rsa_key
.ssh
clear hostkey %d
DISPLAY
%*s %s %s
MIT-MAGIC-COOKIE-1
%02x
Requesting pty.
TERM
ssh.c
Packet integrity error. (%d)
daemon() failed: %.200s
Sending command: %.*s
Requesting shell.
Packet integrity error.
client_init id %d arg %ld
pty-req
auth-agent-req@openssh.com
Sending subsystem: %.*s
subsystem
exec
shell
/dev/null
dup() in/out/err failed
client-session
channel_new: %d
identity file %s type %d
@(#)\$OpenBSD: sshconnect.c,v 1.104 2001/04/12 19:15:25 markus Exp \$
Could not create pipes to communicate with the proxy: %.100s
Executing proxy command: %.500s
ssh_connect: getuid %u geteuid %u anon %d
ssh_connect: getnameinfo failed
Connecting to %.200s [%].100s] port %s.
setsockopt SO_KEEPALIVE: %.100s
ssh_exchange_identification: read: %.100s
ssh_exchange_identification: Connection closed by remote host
ssh_exchange_identification: %s
Bad remote protocol version identification: '%.100s'
Remote protocol version %d.%d, remote software version %.100s

Remote machine has too old SSH software version.
Agent forwarding disabled for protocol 1.3
Protocol major versions differ: %d vs. %d
Forcing accepting of host key for loopback/localhost.
check_host_key: getnameinfo failed
Host '%.200s' is known and matches the %s host key.
Failed to add the %s host key for IP address '%.128s' to the list of known hosts (%.30s).
Warning: Permanently added the %s host key for IP address '%.128s' to the list of known hosts.
No %s host key is known for %.200s and you have requested strict checking.
The authenticity of host '%.200s (%s)' can't be established.
%s key fingerprint is %s.
Are you sure you want to continue connecting (yes/no)?
Failed to add the host to the list of known hosts (%.500s).
Warning: Permanently added '%.200s' (%s) to the list of known hosts.
@@
@ WARNING: POSSIBLE DNS SPOOFING DETECTED! @
The %s host key for %s has changed,
and the key for the according IP address %s
%s. This could either mean that
DNS SPOOFING is happening or the IP address for the host
and its host key have changed at the same time.
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the %s host key has just been changed.
The fingerprint for the %s key sent by the remote host is
Please contact your system administrator.
Add correct host key in %.100s to get rid of this message.
%s host key for %.200s has changed and you have requested strict checking.
Password authentication is disabled to avoid trojan horses.
Agent forwarding is disabled to avoid trojan horses.
X11 forwarding is disabled to avoid trojan horses.
Port forwarding is disabled to avoid trojan horses.
Warning: the %s host key for '%.200s' differs from the key for the IP address '%.128s'
Exiting, you have requested strict checking.
Are you sure you want to continue connecting (yes/no)?
dup2 stdin
dup2 stdout
/bin/sh
fork failed: %.100s
rresvport: af=%d %.100s
Allocated local port %d.
socket: %.100s
%s: %.100s: %s
Trying again...

connect: %.100s
Connection established.
SSH-
SSH-%d.%d-%[^
SSH-%d.%d-%.100s
write: %.100s
Local version string %.100s
/dev/tty
Please type 'yes' or 'no'.
<no hostip for proxy command>
using hostkeyalias: %s
Found key in %s:%d
Aborted by user!
%s,%s
is unknown
is unchanged
has a different value
Offending key for IP in %s:%d
Offending key in %s:%d
Matching host key in %s:%d
@(#)\$OpenBSD: sshconnect1.c,v 1.31 2001/04/17 08:14:01 markus Exp \$
Trying RSA authentication via agent with '%.100s'
Protocol error during RSA authentication: %d
Received RSA challenge from server.
Authentication agent failed to decrypt challenge.
Sending response to RSA challenge.
RSA authentication accepted by server.
Protocol error waiting RSA auth response: %d
RSA authentication using agent refused.
respond_to_rsa_challenge: rsa_private_decrypt failed
respond_to_rsa_challenge: bad challenge length %d
Sending response to host key RSA challenge.
Trying RSA authentication with key '%.100s'
Enter passphrase for RSA key '%.100s':
Will not query passphrase for %.100s in batch mode.
Trying rhosts or /etc/hosts.equiv with RSA host authentication.
Server refused our rhosts authentication or host key.
Received RSA challenge for host key from server.
Rhosts or /etc/hosts.equiv with RSA host authentication accepted by
server.
Rhosts or /etc/hosts.equiv with RSA host authentication refused.
Doing challenge reponse authentication.
Protocol error: got %d in response to SSH_CMSG_AUTH_TIS
Permission denied, please try again.
WARNING: Encryption is disabled! Reponse will be transmitted in clear
text.
Protocol error: got %d in response to SSH_CMSG_AUTH_TIS_RESPONSE
Doing password authentication.
WARNING: Encryption is disabled! Password will be transmitted in clear
text.
Protocol error: got %d in response to passwd auth

Waiting for server public key.

Warning: Server lies about size of server public key: actual size is %d bits vs. announced %d.

Warning: This may be due to an old implementation of ssh.

Warning: Server lies about size of server host key: actual size is %d bits vs. announced %d.

Received server public key (%d bits) and host key (%d bits).

respond_to_rsa_challenge: host_key %d < public_key %d + SSH_KEY_BITS_RESERVED %d

respond_to_rsa_challenge: public_key %d < host_key %d + SSH_KEY_BITS_RESERVED %d

No valid SSH1 cipher, using %.100s instead.

Selected cipher type %.100s not supported by server.

Received encrypted confirmation.

ssh_userauth1: server supports no auth methods

Protocol error: got %d in response to SSH_CMSG_USER

Protocol error: got %d in response to rhosts auth

Server refused our key.

sshconnect1.c

Bad passphrase.

RSA authentication refused.

No challenge.

Response:

%s%s

Encryption type: %.100s

Sent encrypted session key.

Trying rhosts authentication.

%.30s@%.128s's password:

Permission denied.

@(#)\$OpenBSD: sshconnect2.c,v 1.72 2001/04/18 23:43:26 markus Exp \$

hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96

aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael128-cbc,rijndael192-cbc,rij

diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1

No valid ciphers for protocol version 2 given, using defaults.

denied SSH2_MSG_SERVICE_ACCEPT: %d

buggy server: service_accept w/o service

ssh_userauth2: internal error: cannot send userauth none request

ssh-userauth2 successful: method %s

we sent a %s packet, wait for reply

we did not send a packet, disable method

input_userauth_error: bad message during authentication: type %d

input_userauth_success: no authentication context

input_userauth_failure: no authentication context

Authenticated with partial success.

authentications that can continue: %s

input_userauth_pk_ok: no authentication context

input_userauth_pk_ok: SSH_BUG_PKOK

input_userauth_pk_ok: pkalg %s blen %d lastkey %p hint %d

sign_and_send_pubkey: cannot handle key

userauth_pubkey: internal error

send_pubkey_test: cannot handle key

```
Enter passphrase for key '%.100s':
no passphrase given, try next key
bad passphrase given, try again...
userauth_pubkey_agent: no keys at all
userauth_pubkey_agent: no more keys
userauth_pubkey_agent: testing agent key %s
userauth_pubkey_agent: no message sent
input_userauth_info_req: no authentication context
userauth_hostbased: cannot get local ipaddr/name
Unrecognized authentication method name: %s
start over, passed a different list %s
none,zlib
ssh-rsa,ssh-dss
done: ssh_kex2.
hostbased
keyboard-interactive
password
publickey
send SSH2_MSG_SERVICE_REQUEST
ssh-userauth
service_accept: %s
sshconnect2.c
got SSH2_MSG_SERVICE_ACCEPT
ssh-connection
Permission denied (%s).
input_userauth_banner
no last key or no sign cb
unknown pka %s
no key from blob. pka %s
input_userauth_pk_ok: fp %s
key != last_key
clear_auth_state: key_free %p
sign_and_send_pubkey
send_pubkey_test
no such identity: %s
try privkey: %s
try pubkey: %s
userauth_kbdint
input_userauth_info_req
userauth_hostbased: chost %s
xxx: chost %s
key_sign failed
preferred %s
no more auth methods to try
authmethod_lookup %s
remaining preferred: %s
authmethod_is_enabled %s
next auth method to try is %s
tcsetattr
tcgetattr
@(#)OpenBSD: readconf.c,v 1.76 2001/04/17 10:53:25 markus Exp $
```

challengeresponseauthentication

Privileged ports can only be forwarded by root.

Too many local forwards (max %d).

Too many remote forwards (max %d).

%s: line %d: Bad configuration option: %s

%.200s line %d: Missing yes/no argument.

%.200s line %d: Bad yes/no argument.

%.200s line %d: Missing yes/no/ask argument.

%.200s line %d: Bad yes/no/ask argument.

%.200s line %d: Missing argument.

%.200s line %d: Too many identity files specified (max %d).

%.200s line %d: Bad cipher '%s'.

%.200s line %d: Bad SSH2 cipher spec '%s'.

%.200s line %d: Bad SSH2 Mac spec '%s'.

%.200s line %d: Bad protocol 2 host key algorithms '%s'.

%.200s line %d: Bad protocol spec '%s'.

%.200s line %d: unsupported log level '%s'

%.200s line %d: Badly formatted port number.

%.200s line %d: Missing second argument.

%.200s line %d: Badly formatted host:port.

%.200s line %d: Missing port argument.

%.200s line %d: Bad escape character.

process_config_line: Unimplemented opcode %d

%.200s line %d: garbage at end of line; "%.200s".

Reading configuration data %.200s

%s: terminating, %d bad configuration options

hostkeyalgorithms

preferredauthentications

dynamicforward

loglevel

numberofpasswordprompts

keepalive

compressionlevel

compression

stricthostkeychecking

checkhostip

batchmode

connectionattempts

userknownhostsfile2

globalknownhostsfile2

userknownhostsfile

globalknownhostsfile

escapechar

host

user

localforward

remoteforward

protocol

macs

ciphers

cipher

```
proxycommand
hostkeyalias
hostname
identityfile2
identityfile
usersh
fallbacktorsh
tisauthentication
skeyauthentication
hostbasedauthentication
rhostsrsaauthentication
dsaaauthentication
pubkeyauthentication
kbdinteractivedevices
kbdinteractiveauthentication
passwordauthentication
rhostsauthentication
useprivilegedport
gatewayports
xauthlocation
forwardx11
forwardagent
true
false
%.200s line %d: Bad number.
<NONE>
Applying options for %.100s
/usr/X11R6/bin/xauth
.ssh/identity
~/%.100s
.ssh/id_rsa
.ssh/id_dsa
/etc/ssh/ssh_known_hosts
~/.ssh/known_hosts
/etc/ssh/ssh_known_hosts2
~/.ssh/known_hosts2
@(#)$OpenBSD: clientloop.c,v 1.65 2001/04/20 07:17:51 djm Exp $
client_check_window_change: changed
Connection to %.300s closed by remote host.
Read from remote host %.300s: %.100s
Server does not support re-keying
Supported escape sequences:
~. - terminate connection
~R - Request rekey (SSH protocol 2 only)
~^Z - suspend ssh
~# - list forwarded connections
~& - background ssh (when waiting for connections to terminate)
~? - this message
~~ - send the escape character by typing it twice
(Note that escapes are only recognized immediately after newline.)
client_channel_closed: id %d != session_ident %d
```

Write failed flushing stdout buffer.
Write failed flushing stderr buffer.
Transferred: stdin %lu, stdout %lu, stderr %lu bytes in %.1f seconds
Bytes per second: stdin %.1f, stdout %.1f, stderr %.1f
client_request_forwarded_tcpip: listen %s port %d, originator %s port %d
Warning: ssh server tried X11 forwarding.
Warning: this is probably a break in attempt by a malicious server.
buggy server: x11 request w/o originator_port
client_request_x11: request from %s %d
Warning: ssh server tried agent forwarding.
authentication agent connection
client_input_channel_open: ctype %s rchan %d win %d max %d
client_input_channel_req: channel %d rtype %s reply %d
client_input_channel_req: no channel %d
client_input_channel_req: channel %d: wrong channel: %d
client_input_channel_req: channel %d: unknown channel
Killed by signal %d.
Sending eof.
window-change
select: %s
%c^Z [suspend ssh]
%c& [backgrounded]
fork: %.100s
read: %.100s
write stdout: %.50s
Entering interactive session.
rekeying in progress
user requests rekeying
Connection to %.64s closed.
Exit status %d
clientloop.c
forwarded-tcpip
auth-agent@openssh.com
confirm %s
failure %s
bla bla
exit-status
@(#)OpenBSD: atomicio.c,v 1.9 2001/03/02 18:54:30 deraadt Exp \$
@(#)OpenBSD: authfd.c,v 1.39 2001/04/05 10:42:48 markus Exp \$
Error writing to authentication socket.
Error reading response length from authentication socket.
Authentication response too long: %d
Error reading response from authentication socket.
Bad authentication reply message type: %d
Too many identities in authentication reply: %d
Warning: identity keysize mismatch: actual %d, announced %u
Compatibility with ssh protocol version 1.0 no longer supported.
Agent admitted failure to authenticate using the key.
Bad authentication response: %d
Agent admitted failure to sign using the key.

```
Bad response from authentication agent: %d
SSH_AUTH_SOCK
SSH_AGENT_FAILURE
@(#)$OpenBSD: authfile.c,v 1.32 2001/04/18 23:44:51 markus Exp $
save_private_key_rsa: bad cipher
write to key file %s failed: %s
passphrase too short: have %d bytes, need > 4
key_save_private: cannot save key type %d
Read from key file %.200s failed: %.100s
Unsupported cipher %d used in key file %.200s.
Bad passphrase supplied for key file %.200s.
PEM_read_PrivateKey: mismatch or unknown EVP_PKEY save_type %d
read PEM private key done: type %s
@ WARNING: UNPROTECTED PRIVATE KEY FILE! @
Bad ownership or mode(0%3.3o) for '%s'.
It is recommended that your private key files are NOT accessible by
others.
This private key will be ignored.
bad permissions: ignore key: %s
fdopen %s failed: %s.
No RSA1 key file %.200s.
<no key>
fdopen failed: %s
PEM_read_PrivateKey failed
rsa w/o comment
dsa w/o comment
<unknown>
.pub
@(#)$OpenBSD: bufaux.c,v 1.17 2001/01/21 19:05:45 markus Exp $
buffer_put_bignum: BN_bn2bin() failed: oi %d != bin_size %d
buffer_get_bignum: input buffer too small
Received packet with bad string length %d
negativ!
@(#)$OpenBSD: buffer.c,v 1.13 2001/04/12 19:15:24 markus Exp $
buffer_get: trying to get more bytes %d than in buffer %d
buffer_consume: trying to get more bytes than in buffer
buffer_consume_end: trying to get more bytes than in buffer
@(#)$OpenBSD: canohost.c,v 1.26 2001/04/18 14:15:00 markus Exp $
get_remote_hostname: getnameinfo NI_NUMERICHOST failed
Trying to reverse map address %.100s.
Could not reverse map address %.100s.
reverse mapping checking getaddrinfo for %.700s failed – POSSIBLE
BREAKIN ATTEMPT!
Address %.100s maps to %.600s, but this does not map back to the
address – POSSIBLE BREAKIN ATTEMPT!
Connection from %.100s with IP options:%.800s
get_socket_ipaddr: getpeername failed: %.100s
get_socket_ipaddr: getsockname failed: %.100s
get_socket_ipaddr: getnameinfo %d failed
get_sock_port: getnameinfo NI_NUMERICSERV failed
getpeername failed: %.100s
```

%2.2x

- *Next message:* [Yan Seiner: "Re: understanding chkrootkit: sshd section"](#)
- *Previous message:* [Ed Turner: "Re: ftp was hacked"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)