NETWORK RESEARCH (REMOTE CONTROL)

Yap Ching Siong
CFC2407

Contents

Overview of the script

This script is created to allow local machine to access remote server (SSH server in this script), then perform nmap, masscan, and whois scan from the remote server.

The scanned results will be copy back to local machine, and remove from the remote server.

The assumption for this script is that both local machine and remote server does not have the tools/updates installed for all tasks.

NOTE: User inputs are required throughout the execution of this script.

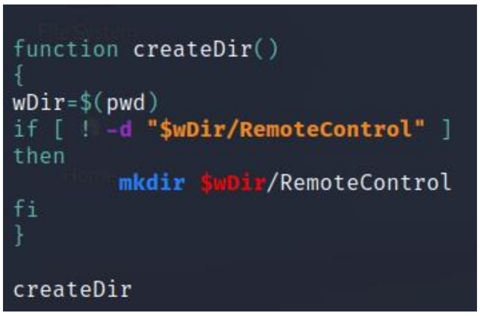
inst function will perform Tools update and installation on local machine.

anon function will activate Nipe, check identity of local machine to ensure it is anonymous(not from SG),

Detail code explanation will be in the following section.

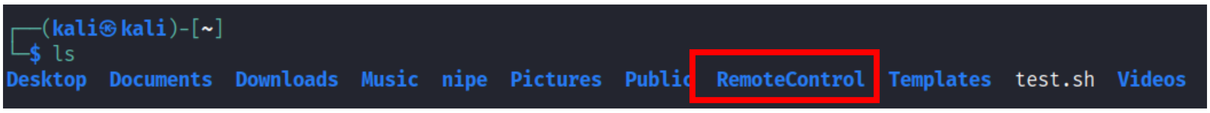
createDir function

The createDir function creates a directory to store saved results from the remote control scans.



```
function createDir()
{
wDir=$(pwd)
if [ ! -d "$wDir/RemoteControl" ]
then
        mkdir $wDir/RemoteControl
fi
}

createDir
```

```
# Start createDir function

function createDir()

{


# Check the present working directory and store path string in wDir variable. This variable will be
#  used often throughout this script for accessing directories to save logs and results.

wDir=$(pwd)


# -d flag to check for existence of folder.

# ! in if condition to check that the folder does not exist.

# then mkdir to create RemoteControl folder in present working directory .

if [ ! -d "$wDir/RemoteControl" ]

then

        mkdir $wDir/RemoteControl

fi

}
```

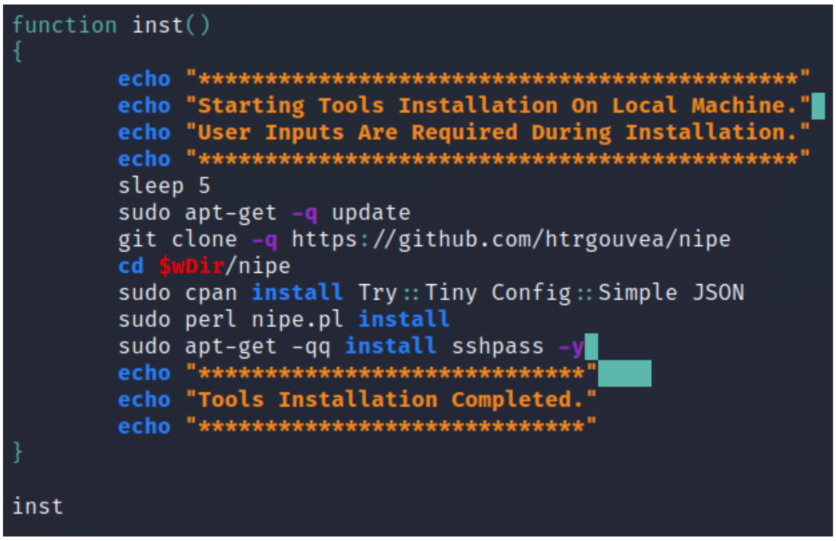


```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  nipe  Pictures  Public  RemoteControl  Templates  test.sh  Videos
```

inst function

The inst function will execute the following actions:

1. apt-get update
2. nipe installation



```
function inst()
{
        echo "*********************************************"
        echo "Starting Tools Installation On Local Machine."
        echo "User Inputs Are Required During Installation."
        echo "*********************************************"
        sleep 5
        sudo apt-get -q update
        git clone -q https://github.com/htrgouvea/nipe
        cd $wDir/nipe
        sudo cpan install Try::Tiny Config::Simple JSON
        sudo perl nipe.pl install
        sudo apt-get -qq install sshpass -y
        echo "*****************************"
        echo "Tools Installation Completed."
        echo "*****************************"
}

inst
```

```
# Start of inst function

function inst()

{


# Notify user tools installation will be starting and user should provide inputs when asked, follow by
# a sleep command, which means wait for 5 seconds before running the next line of the script.

echo "*********************************************"

echo "Starting Tools Installation On Local Machine."

echo "User Inputs Are Required During Installation."

echo "*********************************************"

sleep 5
```

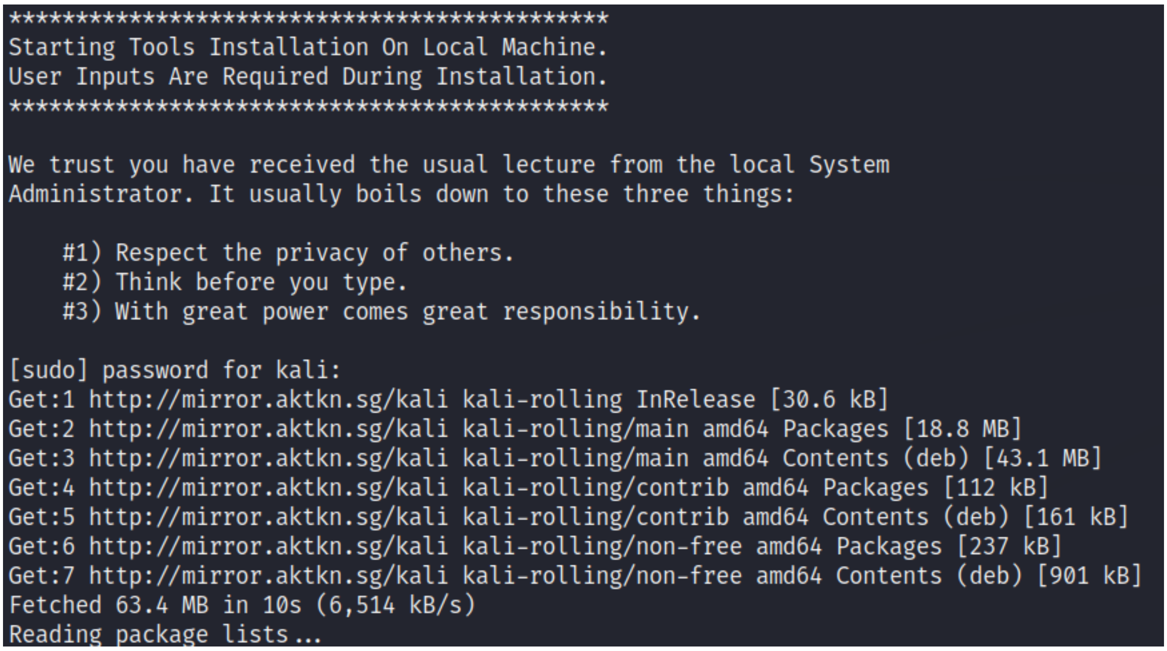
# sudo = superuser doer, used in front of a command to execute normal user command with root
# privileges without changing to root user. sudo is used because some commands require elevated
# permission.

# apt-get update, downloads versions of updated package information or their dependencies to
# local machine.

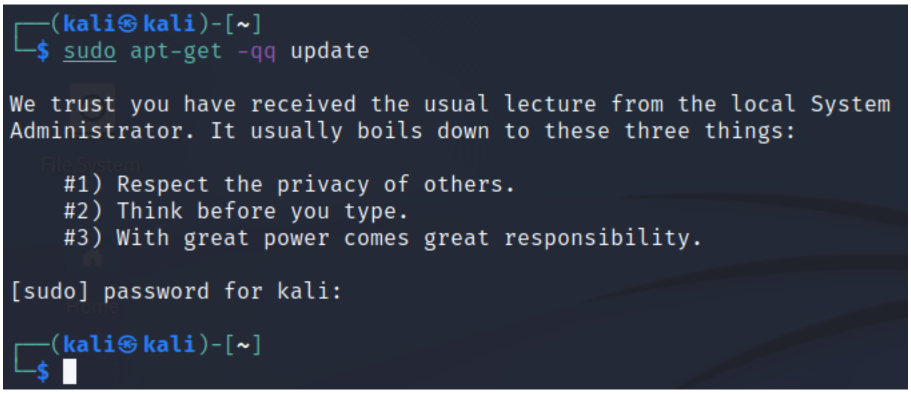
# -q , display output suitable for logging on terminal and omit progress indicators.

# -qq can be used to set maximum quiet level, no output will be displayed on the terminal.

sudo apt-get -q update



```
*********************************************
Starting Tools Installation On Local Machine.
User Inputs Are Required During Installation.
*********************************************

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
Get:1 http://mirror.aktkn.sg/kali kali-rolling InRelease [30.6 kB]
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Packages [18.8 MB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Contents (deb) [43.1 MB]
Get:4 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Contents (deb) [161 kB]
Get:6 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Packages [237 kB]
Get:7 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Contents (deb) [901 kB]
Fetched 63.4 MB in 10s (6,514 kB/s)
Reading package lists...
```



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get -qq update

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ █
```

# Difference between -q and -qq, in the script -q is use to display progress of the update to user.

# quiet cloning of files required for installing nipe from https://github.com/htrgouvea/nipe, follow
# by changing directory into nipe folder

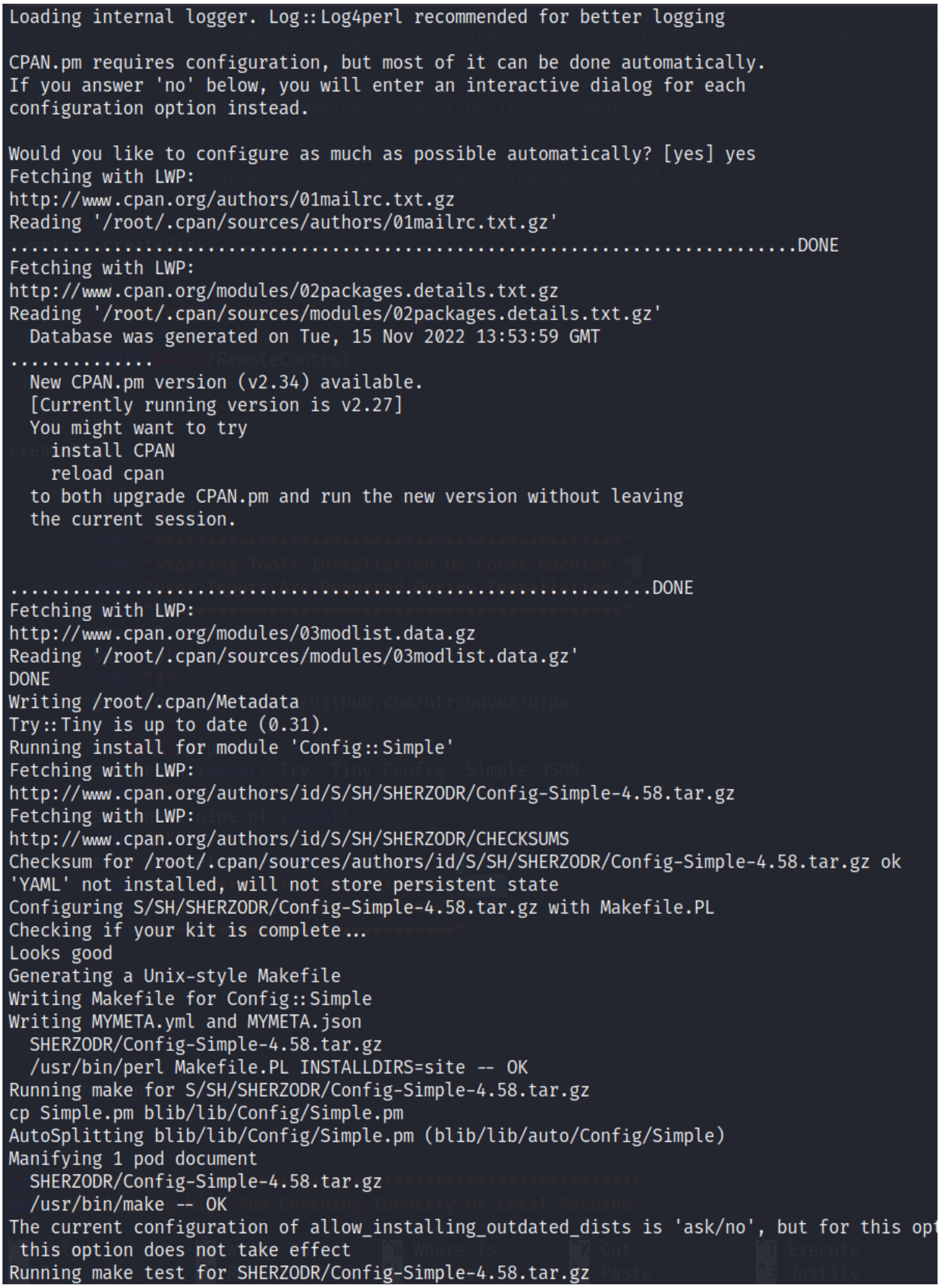
git clone -q https://github.com/htrgouvea/nipe

# cd into nipe folder

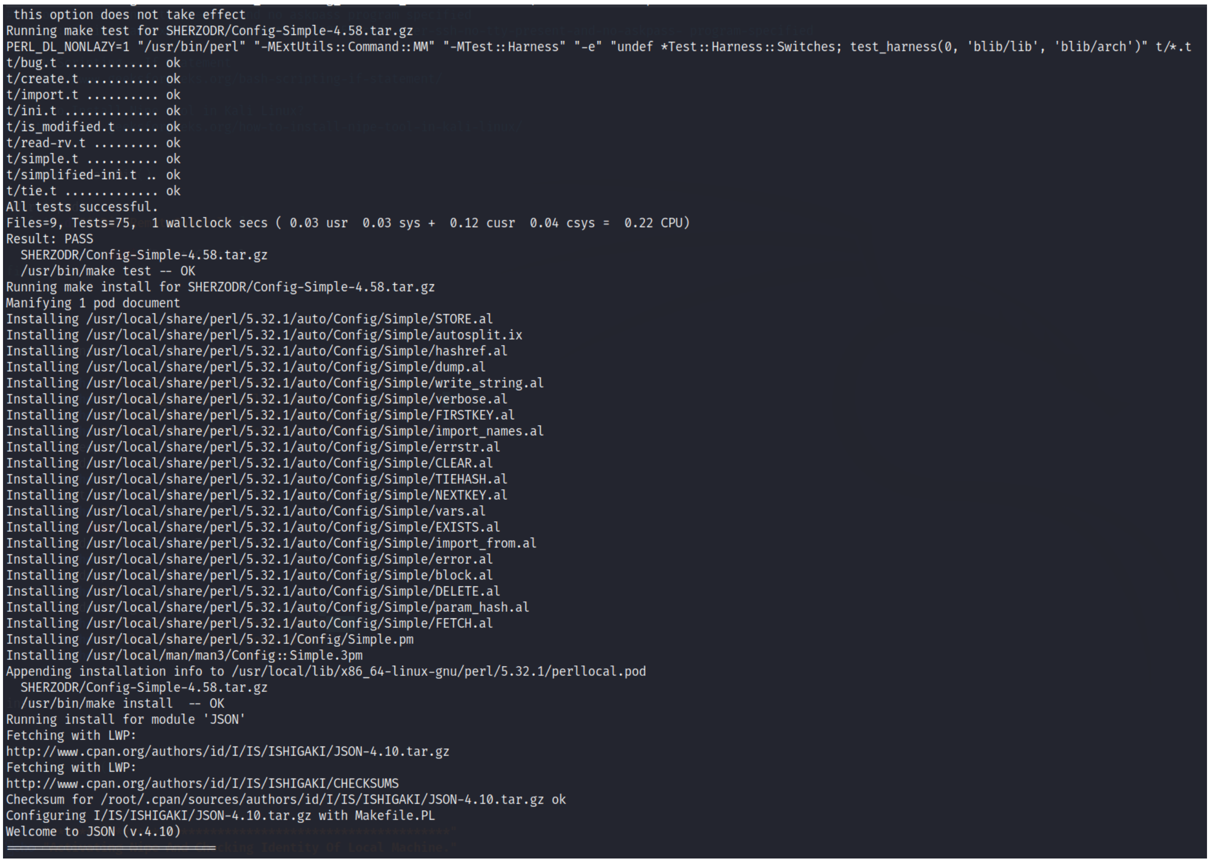
# install lib and dependencies from cpan repository inside nipe folder

cd $wDir/nipe

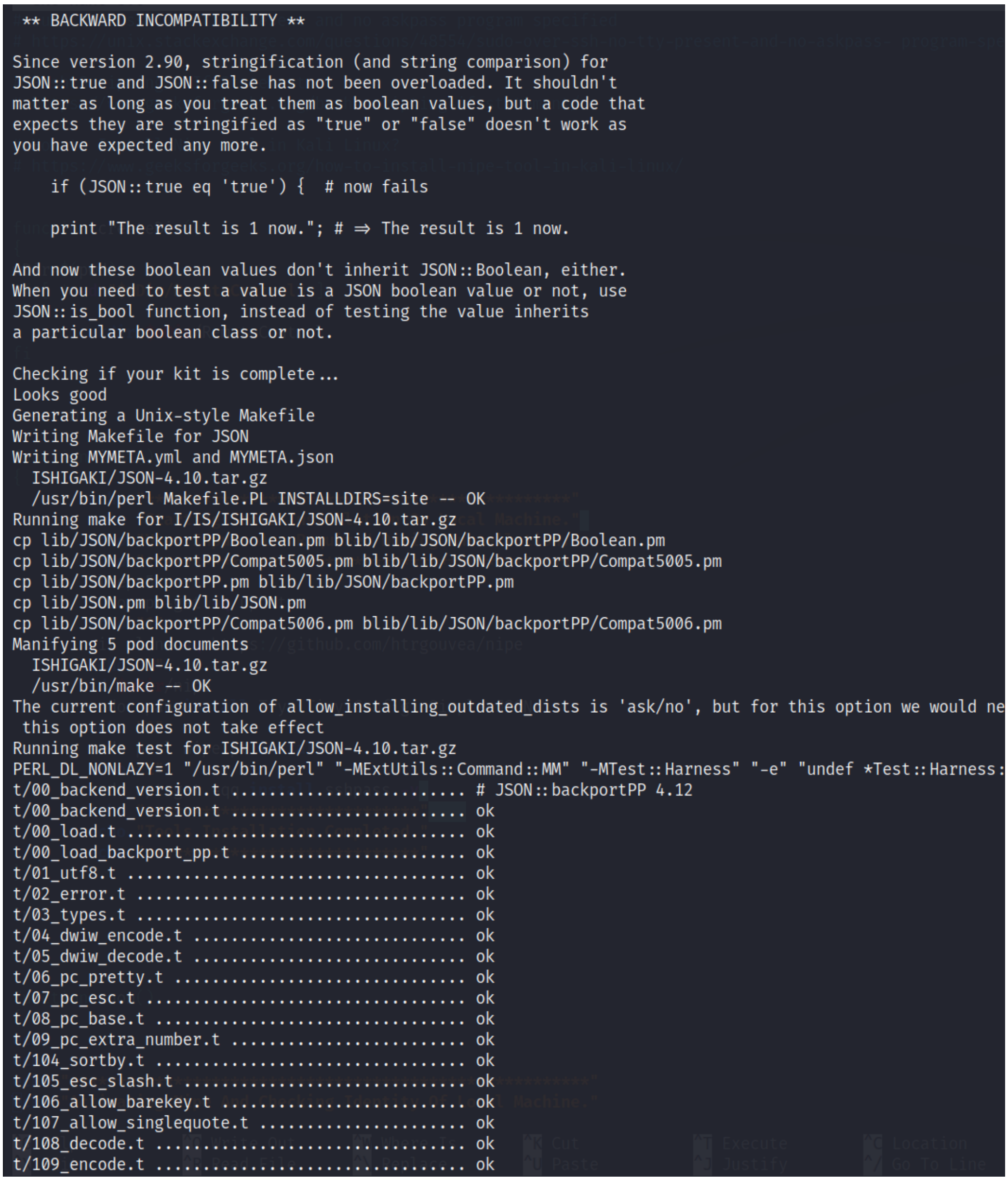
sudo cpan install Try::Tiny Config::Simple JSON



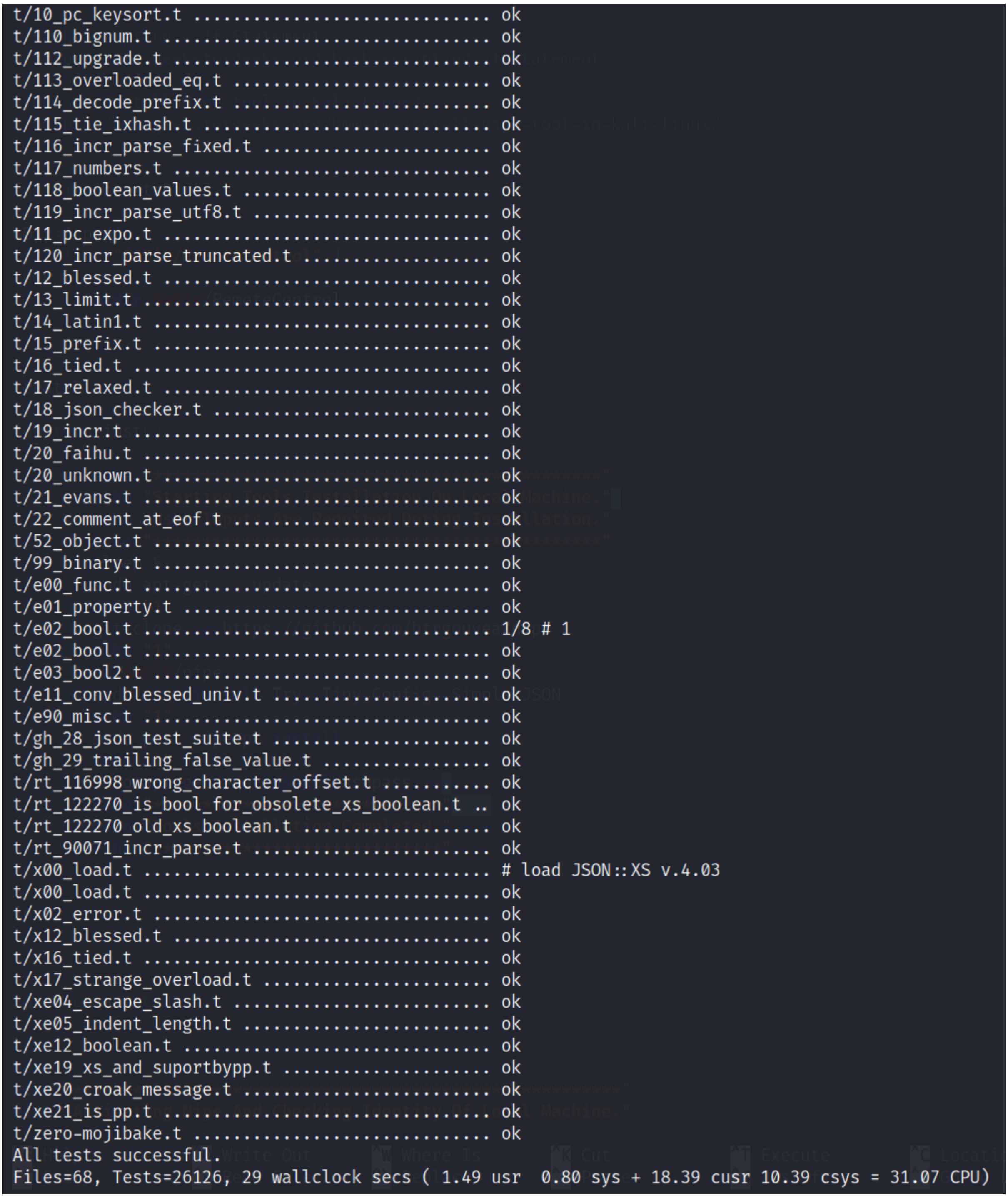
```
Loading internal logger. Log::Log4perl recommended for better logging

CPAN.pm requires configuration, but most of it can be done automatically.
If you answer 'no' below, you will enter an interactive dialog for each
configuration option instead.

Would you like to configure as much as possible automatically? [yes] yes
Fetching with LWP:
http://www.cpan.org/authors/01mailrc.txt.gz
Reading '/root/.cpan/sources/authors/01mailrc.txt.gz'
............................................................................DONE
Fetching with LWP:
http://www.cpan.org/modules/02packages.details.txt.gz
Reading '/root/.cpan/sources/modules/02packages.details.txt.gz'
  Database was generated on Tue, 15 Nov 2022 13:53:59 GMT
..............
  New CPAN.pm version (v2.34) available.
  [Currently running version is v2.27]
  You might want to try
    install CPAN
    reload cpan
  to both upgrade CPAN.pm and run the new version without leaving
  the current session.


..............................................................DONE
Fetching with LWP:
http://www.cpan.org/modules/03modlist.data.gz
Reading '/root/.cpan/sources/modules/03modlist.data.gz'
DONE
Writing /root/.cpan/Metadata
Try::Tiny is up to date (0.31).
Running install for module 'Config::Simple'
Fetching with LWP:
http://www.cpan.org/authors/id/S/SH/SHERZODR/Config-Simple-4.58.tar.gz
Fetching with LWP:
http://www.cpan.org/authors/id/S/SH/SHERZODR/CHECKSUMS
Checksum for /root/.cpan/sources/authors/id/S/SH/SHERZODR/Config-Simple-4.58.tar.gz ok
'YAML' not installed, will not store persistent state
Configuring S/SH/SHERZODR/Config-Simple-4.58.tar.gz with Makefile.PL
Checking if your kit is complete...
Looks good
Generating a Unix-style Makefile
Writing Makefile for Config::Simple
Writing MYMETA.yml and MYMETA.json
  SHERZODR/Config-Simple-4.58.tar.gz
  /usr/bin/perl Makefile.PL INSTALLDIRS=site -- OK
Running make for S/SH/SHERZODR/Config-Simple-4.58.tar.gz
cp Simple.pm blib/lib/Config/Simple.pm
AutoSplitting blib/lib/Config/Simple.pm (blib/lib/auto/Config/Simple)
Manifying 1 pod document
  SHERZODR/Config-Simple-4.58.tar.gz
  /usr/bin/make -- OK
The current configuration of allow_installing_outdated_dists is 'ask/no', but for this opt
 this option does not take effect
Running make test for SHERZODR/Config-Simple-4.58.tar.gz
```



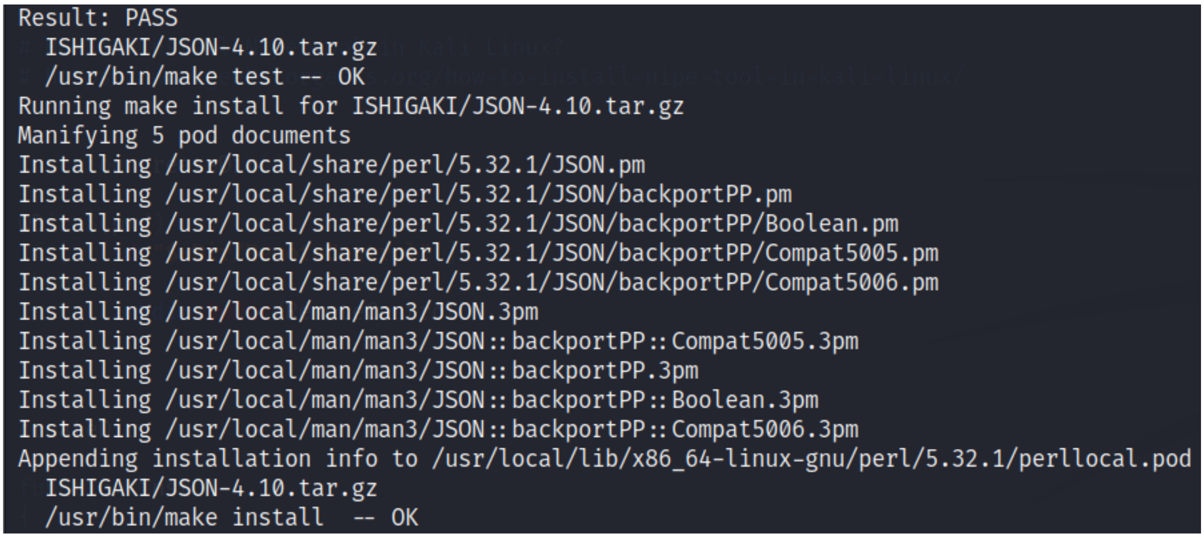
```
 this option does not take effect
Running make test for SHERZODR/Config-Simple-4.58.tar.gz
PERL_DL_NONLAZY=1 "/usr/bin/perl" "-MExtUtils::Command::MM" "-MTest::Harness" "-e" "undef *Test::Harness::Switches; test_harness(0, 'blib/lib', 'blib/arch')" t/*.t
t/bug.t ............ ok
t/create.t ......... ok
t/import.t ......... ok
t/ini.t ............ ok
t/is_modified.t ..... ok
t/read-rv.t ......... ok
t/simple.t ......... ok
t/simplified-ini.t .. ok
t/tie.t ............ ok
All tests successful.
Files=9, Tests=75,  1 wallclock secs ( 0.03 usr  0.03 sys +  0.12 cusr  0.04 csys =  0.22 CPU)
Result: PASS
  SHERZODR/Config-Simple-4.58.tar.gz
  /usr/bin/make test -- OK
Running make install for SHERZODR/Config-Simple-4.58.tar.gz
Manifying 1 pod document
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/STORE.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/autosplit.ix
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/hashref.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/dump.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/write_string.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/verbose.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/FIRSTKEY.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/import_names.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/errstr.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/CLEAR.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/TIEHASH.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/NEXTKEY.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/vars.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/EXISTS.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/import_from.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/error.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/block.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/DELETE.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/param_hash.al
Installing /usr/local/share/perl/5.32.1/auto/Config/Simple/FETCH.al
Installing /usr/local/share/perl/5.32.1/Config/Simple.pm
Installing /usr/local/man/man3/Config::Simple.3pm
Appending installation info to /usr/local/lib/x86_64-linux-gnu/perl/5.32.1/perllocal.pod
  SHERZODR/Config-Simple-4.58.tar.gz
  /usr/bin/make install  -- OK
Running install for module 'JSON'
Fetching with LWP:
http://www.cpan.org/authors/id/I/IS/ISHIGAKI/JSON-4.10.tar.gz
Fetching with LWP:
http://www.cpan.org/authors/id/I/IS/ISHIGAKI/CHECKSUMS
Checksum for /root/.cpan/sources/authors/id/I/IS/ISHIGAKI/JSON-4.10.tar.gz ok
Configuring I/IS/ISHIGAKI/JSON-4.10.tar.gz with Makefile.PL
Welcome to JSON (v.4.10)
═════════════════════════════
```



```
 ** BACKWARD INCOMPATIBILITY **

Since version 2.90, stringification (and string comparison) for
JSON::true and JSON::false has not been overloaded. It shouldn't
matter as long as you treat them as boolean values, but a code that
expects they are stringified as "true" or "false" doesn't work as
you have expected any more.

    if (JSON::true eq 'true') {  # now fails

    print "The result is 1 now."; # => The result is 1 now.

And now these boolean values don't inherit JSON::Boolean, either.
When you need to test a value is a JSON boolean value or not, use
JSON::is_bool function, instead of testing the value inherits
a particular boolean class or not.

Checking if your kit is complete...
Looks good
Generating a Unix-style Makefile
Writing Makefile for JSON
Writing MYMETA.yml and MYMETA.json
  ISHIGAKI/JSON-4.10.tar.gz
  /usr/bin/perl Makefile.PL INSTALLDIRS=site -- OK
Running make for I/IS/ISHIGAKI/JSON-4.10.tar.gz
cp lib/JSON/backportPP/Boolean.pm blib/lib/JSON/backportPP/Boolean.pm
cp lib/JSON/backportPP/Compat5005.pm blib/lib/JSON/backportPP/Compat5005.pm
cp lib/JSON/backportPP.pm blib/lib/JSON/backportPP.pm
cp lib/JSON.pm blib/lib/JSON.pm
cp lib/JSON/backportPP/Compat5006.pm blib/lib/JSON/backportPP/Compat5006.pm
Manifying 5 pod documents
  ISHIGAKI/JSON-4.10.tar.gz
  /usr/bin/make -- OK
The current configuration of allow_installing_outdated_dists is 'ask/no', but for this option we would ne
 this option does not take effect
Running make test for ISHIGAKI/JSON-4.10.tar.gz
PERL_DL_NONLAZY=1 "/usr/bin/perl" "-MExtUtils::Command::MM" "-MTest::Harness" "-e" "undef *Test::Harness:
t/00_backend_version.t ......................... # JSON::backportPP 4.12
t/00_backend_version.t ......................... ok
t/00_load.t .................................... ok
t/00_load_backport_pp.t ........................ ok
t/01_utf8.t .................................... ok
t/02_error.t ................................... ok
t/03_types.t ................................... ok
t/04_dwiw_encode.t ............................. ok
t/05_dwiw_decode.t ............................. ok
t/06_pc_pretty.t ............................... ok
t/07_pc_esc.t .................................. ok
t/08_pc_base.t ................................. ok
t/09_pc_extra_number.t ......................... ok
t/104_sortby.t ................................. ok
t/105_esc_slash.t .............................. ok
t/106_allow_barekey.t .......................... ok
t/107_allow_singlequote.t ...................... ok
t/108_decode.t ................................. ok
t/109_encode.t ................................. ok
```



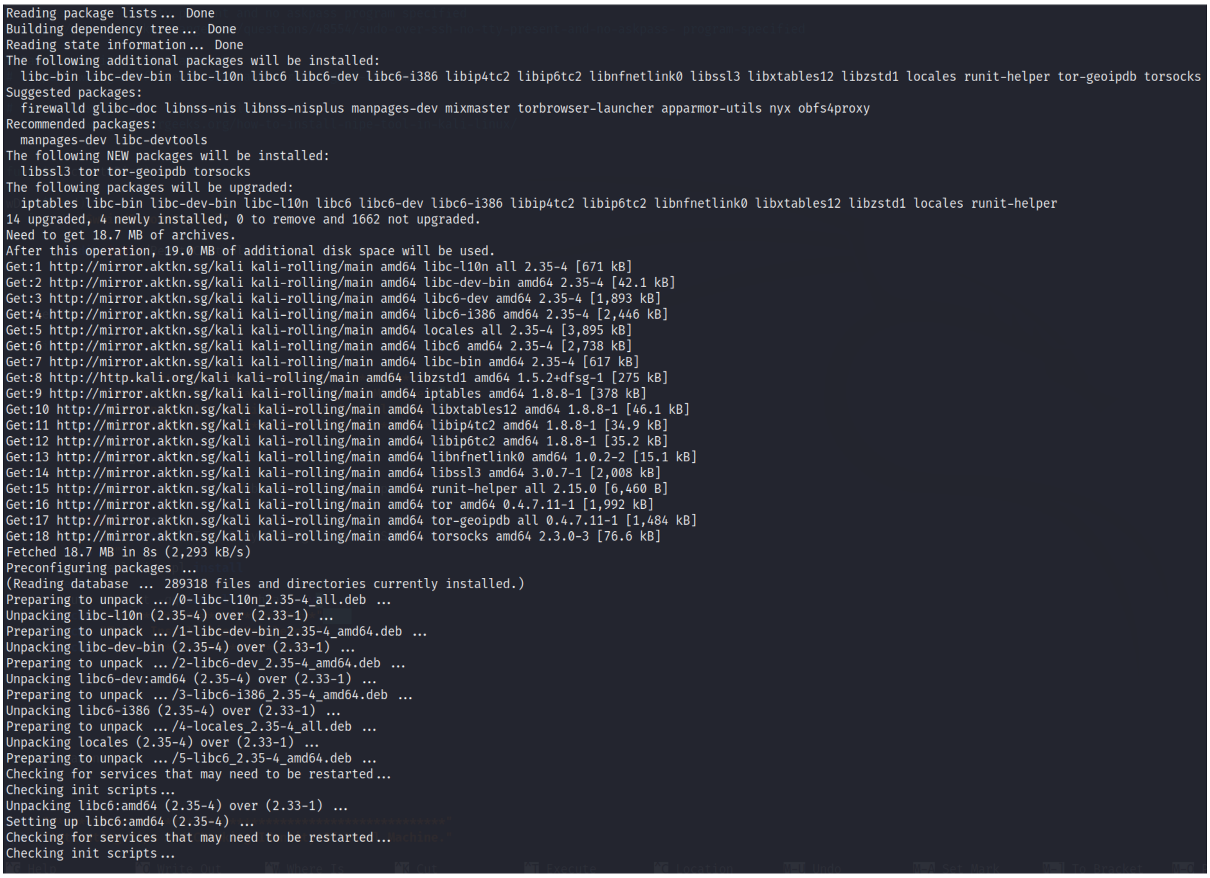
```
t/10_pc_keysort.t ............................... ok
t/110_bignum.t .................................. ok
t/112_upgrade.t ................................. ok
t/113_overloaded_eq.t ........................... ok
t/114_decode_prefix.t ........................... ok
t/115_tie_ixhash.t .............................. ok
t/116_incr_parse_fixed.t ........................ ok
t/117_numbers.t ................................. ok
t/118_boolean_values.t .......................... ok
t/119_incr_parse_utf8.t ......................... ok
t/11_pc_expo.t .................................. ok
t/120_incr_parse_truncated.t .................... ok
t/12_blessed.t .................................. ok
t/13_limit.t .................................... ok
t/14_latin1.t ................................... ok
t/15_prefix.t ................................... ok
t/16_tied.t ..................................... ok
t/17_relaxed.t .................................. ok
t/18_json_checker.t ............................. ok
t/19_incr.t ..................................... ok
t/20_faihu.t .................................... ok
t/20_unknown.t .................................. ok
t/21_evans.t .................................... ok
t/22_comment_at_eof.t ........................... ok
t/52_object.t ................................... ok
t/99_binary.t ................................... ok
t/e00_func.t .................................... ok
t/e01_property.t ................................ ok
t/e02_bool.t .................................... 1/8 # 1
t/e02_bool.t .................................... ok
t/e03_bool2.t ................................... ok
t/e11_conv_blessed_univ.t ....................... ok
t/e90_misc.t .................................... ok
t/gh_28_json_test_suite.t ....................... ok
t/gh_29_trailing_false_value.t .................. ok
t/rt_116998_wrong_character_offset.t ............ ok
t/rt_122270_is_bool_for_obsolete_xs_boolean.t .. ok
t/rt_122270_old_xs_boolean.t .................... ok
t/rt_90071_incr_parse.t ......................... ok
t/x00_load.t .................................... # load JSON::XS v.4.03
t/x00_load.t .................................... ok
t/x02_error.t ................................... ok
t/x12_blessed.t ................................. ok
t/x16_tied.t .................................... ok
t/x17_strange_overload.t ........................ ok
t/xe04_escape_slash.t ........................... ok
t/xe05_indent_length.t .......................... ok
t/xe12_boolean.t ................................ ok
t/xe19_xs_and_suportbypp.t ...................... ok
t/xe20_croak_message.t .......................... ok
t/xe21_is_pp.t .................................. ok
t/zero-mojibake.t ............................... ok
All tests successful.
Files=68, Tests=26126, 29 wallclock secs ( 1.49 usr  0.80 sys + 18.39 cusr 10.39 csys = 31.07 CPU)
```



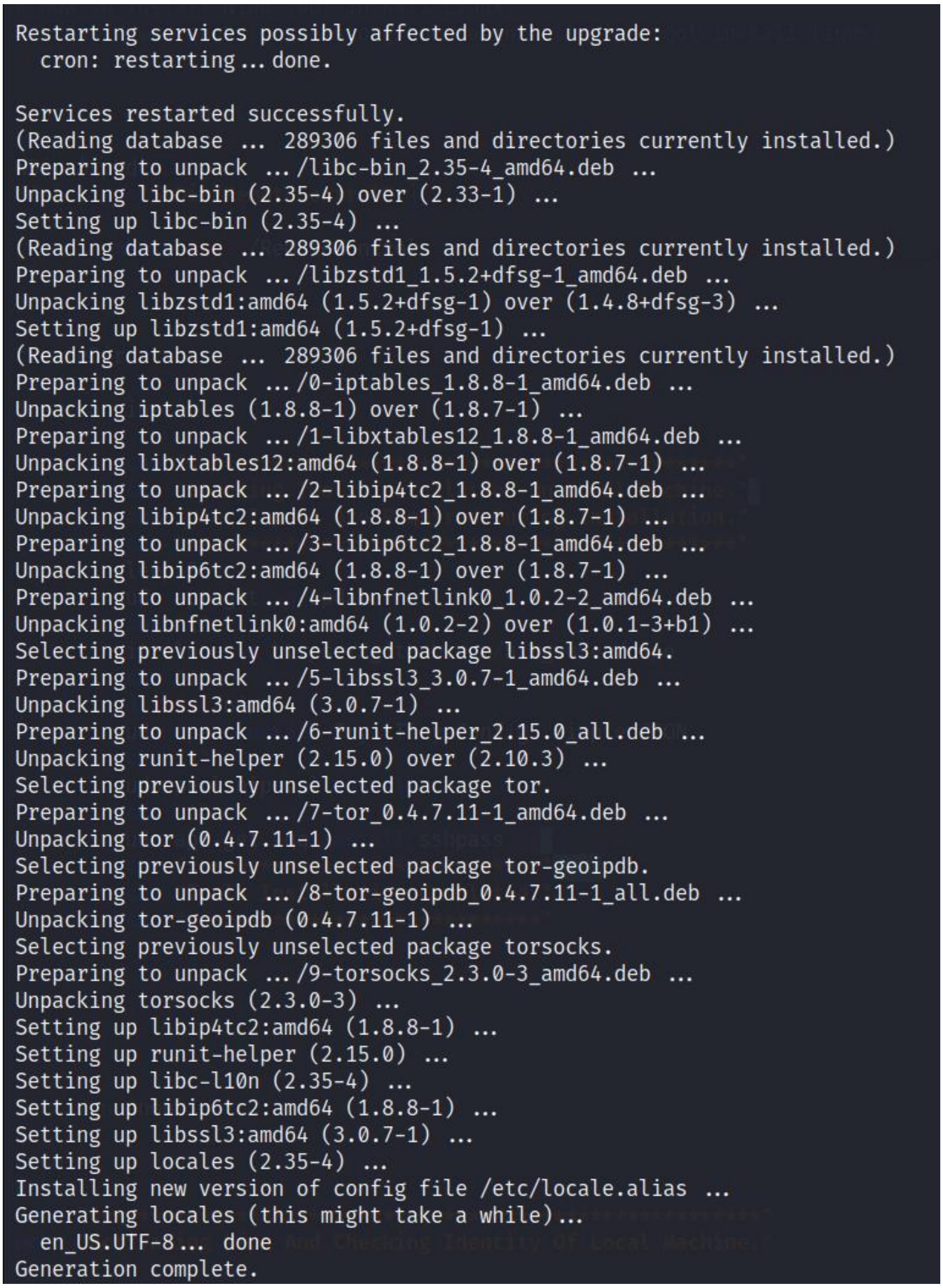
```
Result: PASS
  ISHIGAKI/JSON-4.10.tar.gz
  /usr/bin/make test -- OK
Running make install for ISHIGAKI/JSON-4.10.tar.gz
Manifying 5 pod documents
Installing /usr/local/share/perl/5.32.1/JSON.pm
Installing /usr/local/share/perl/5.32.1/JSON/backportPP.pm
Installing /usr/local/share/perl/5.32.1/JSON/backportPP/Boolean.pm
Installing /usr/local/share/perl/5.32.1/JSON/backportPP/Compat5005.pm
Installing /usr/local/share/perl/5.32.1/JSON/backportPP/Compat5006.pm
Installing /usr/local/man/man3/JSON.3pm
Installing /usr/local/man/man3/JSON::backportPP::Compat5005.3pm
Installing /usr/local/man/man3/JSON::backportPP.3pm
Installing /usr/local/man/man3/JSON::backportPP::Boolean.3pm
Installing /usr/local/man/man3/JSON::backportPP::Compat5006.3pm
Appending installation info to /usr/local/lib/x86_64-linux-gnu/perl/5.32.1/perllocal.pod
  ISHIGAKI/JSON-4.10.tar.gz
  /usr/bin/make install  -- OK
```

# execute perl script ‘nipe.pl’ to install nipe

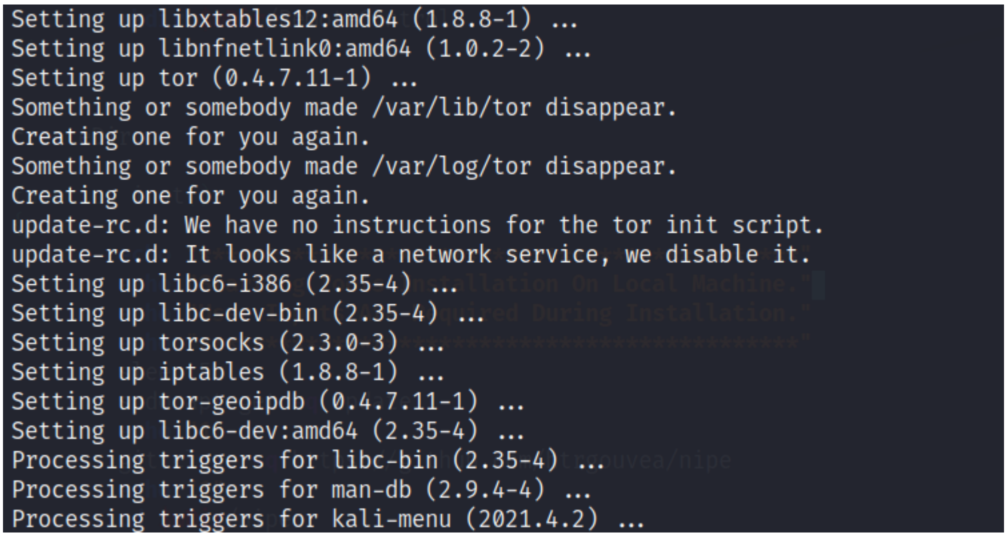
sudo perl nipe.pl install



```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libip4tc2 libip6tc2 libnfnetlink0 libssl3 libxtables12 libzstd1 locales runit-helper tor-geoipdb torsocks
Suggested packages:
  firewalld glibc-doc libnss-nis libnss-nisplus manpages-dev mixmaster torbrowser-launcher apparmor-utils nyx obfs4proxy
Recommended packages:
  manpages-dev libc-devtools
The following NEW packages will be installed:
  libssl3 tor tor-geoipdb torsocks
The following packages will be upgraded:
  iptables libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libip4tc2 libip6tc2 libnfnetlink0 libxtables12 libzstd1 locales runit-helper
14 upgraded, 4 newly installed, 0 to remove and 1662 not upgraded.
Need to get 18.7 MB of archives.
After this operation, 19.0 MB of additional disk space will be used.
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libc-l10n all 2.35-4 [671 kB]
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libc-dev-bin amd64 2.35-4 [42.1 kB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libc6-dev amd64 2.35-4 [1,893 kB]
Get:4 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libc6-i386 amd64 2.35-4 [2,446 kB]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/main amd64 locales all 2.35-4 [3,895 kB]
Get:6 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libc6 amd64 2.35-4 [2,738 kB]
Get:7 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libc-bin amd64 2.35-4 [617 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 libzstd1 amd64 1.5.2+dfsg-1 [275 kB]
Get:9 http://mirror.aktkn.sg/kali kali-rolling/main amd64 iptables amd64 1.8.8-1 [378 kB]
Get:10 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libxtables12 amd64 1.8.8-1 [46.1 kB]
Get:11 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libip4tc2 amd64 1.8.8-1 [34.9 kB]
Get:12 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libip6tc2 amd64 1.8.8-1 [35.2 kB]
Get:13 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libnfnetlink0 amd64 1.0.2-2 [15.1 kB]
Get:14 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libssl3 amd64 3.0.7-1 [2,008 kB]
Get:15 http://mirror.aktkn.sg/kali kali-rolling/main amd64 runit-helper all 2.15.0 [6,460 B]
Get:16 http://mirror.aktkn.sg/kali kali-rolling/main amd64 tor amd64 0.4.7.11-1 [1,992 kB]
Get:17 http://mirror.aktkn.sg/kali kali-rolling/main amd64 tor-geoipdb all 0.4.7.11-1 [1,484 kB]
Get:18 http://mirror.aktkn.sg/kali kali-rolling/main amd64 torsocks amd64 2.3.0-3 [76.6 kB]
Fetched 18.7 MB in 8s (2,293 kB/s)
Preconfiguring packages ...
(Reading database ... 289318 files and directories currently installed.)
Preparing to unpack .../0-libc-l10n_2.35-4_all.deb ...
Unpacking libc-l10n (2.35-4) over (2.33-1) ...
Preparing to unpack .../1-libc-dev-bin_2.35-4_amd64.deb ...
Unpacking libc-dev-bin (2.35-4) over (2.33-1) ...
Preparing to unpack .../2-libc6-dev_2.35-4_amd64.deb ...
Unpacking libc6-dev:amd64 (2.35-4) over (2.33-1) ...
Preparing to unpack .../3-libc6-i386_2.35-4_amd64.deb ...
Unpacking libc6-i386 (2.35-4) over (2.33-1) ...
Preparing to unpack .../4-locales_2.35-4_all.deb ...
Unpacking locales (2.35-4) over (2.33-1) ...
Preparing to unpack .../5-libc6_2.35-4_amd64.deb ...
Checking for services that may need to be restarted...
Checking init scripts...
Unpacking libc6:amd64 (2.35-4) over (2.33-1) ...
Setting up libc6:amd64 (2.35-4) ...
Checking for services that may need to be restarted...
Checking init scripts...
```



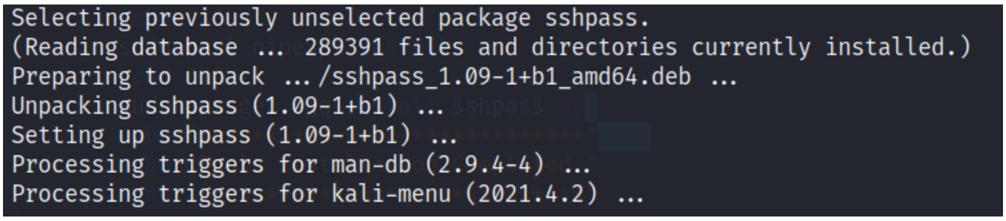
```
Restarting services possibly affected by the upgrade:
  cron: restarting... done.

Services restarted successfully.
(Reading database ... 289306 files and directories currently installed.)
Preparing to unpack .../libc-bin_2.35-4_amd64.deb ...
Unpacking libc-bin (2.35-4) over (2.33-1) ...
Setting up libc-bin (2.35-4) ...
(Reading database ... 289306 files and directories currently installed.)
Preparing to unpack .../libzstd1_1.5.2+dfsg-1_amd64.deb ...
Unpacking libzstd1:amd64 (1.5.2+dfsg-1) over (1.4.8+dfsg-3) ...
Setting up libzstd1:amd64 (1.5.2+dfsg-1) ...
(Reading database ... 289306 files and directories currently installed.)
Preparing to unpack .../0-iptables_1.8.8-1_amd64.deb ...
Unpacking iptables (1.8.8-1) over (1.8.7-1) ...
Preparing to unpack .../1-libxtables12_1.8.8-1_amd64.deb ...
Unpacking libxtables12:amd64 (1.8.8-1) over (1.8.7-1) ...
Preparing to unpack .../2-libip4tc2_1.8.8-1_amd64.deb ...
Unpacking libip4tc2:amd64 (1.8.8-1) over (1.8.7-1) ...
Preparing to unpack .../3-libip6tc2_1.8.8-1_amd64.deb ...
Unpacking libip6tc2:amd64 (1.8.8-1) over (1.8.7-1) ...
Preparing to unpack .../4-libnfnetlink0_1.0.2-2_amd64.deb ...
Unpacking libnfnetlink0:amd64 (1.0.2-2) over (1.0.1-3+b1) ...
Selecting previously unselected package libssl3:amd64.
Preparing to unpack .../5-libssl3_3.0.7-1_amd64.deb ...
Unpacking libssl3:amd64 (3.0.7-1) ...
Preparing to unpack .../6-runit-helper_2.15.0_all.deb ...
Unpacking runit-helper (2.15.0) over (2.10.3) ...
Selecting previously unselected package tor.
Preparing to unpack .../7-tor_0.4.7.11-1_amd64.deb ...
Unpacking tor (0.4.7.11-1) ...
Selecting previously unselected package tor-geoipdb.
Preparing to unpack .../8-tor-geoipdb_0.4.7.11-1_all.deb ...
Unpacking tor-geoipdb (0.4.7.11-1) ...
Selecting previously unselected package torsocks.
Preparing to unpack .../9-torsocks_2.3.0-3_amd64.deb ...
Unpacking torsocks (2.3.0-3) ...
Setting up libip4tc2:amd64 (1.8.8-1) ...
Setting up runit-helper (2.15.0) ...
Setting up libc-l10n (2.35-4) ...
Setting up libip6tc2:amd64 (1.8.8-1) ...
Setting up libssl3:amd64 (3.0.7-1) ...
Setting up locales (2.35-4) ...
Installing new version of config file /etc/locale.alias ...
Generating locales (this might take a while)...
  en_US.UTF-8... done
Generation complete.
```



```
Setting up libxtables12:amd64 (1.8.8-1) ...
Setting up libnfnetlink0:amd64 (1.0.2-2) ...
Setting up tor (0.4.7.11-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
Something or somebody made /var/log/tor disappear.
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up libc6-i386 (2.35-4) ...
Setting up libc-dev-bin (2.35-4) ...
Setting up torsocks (2.3.0-3) ...
Setting up iptables (1.8.8-1) ...
Setting up tor-geoipdb (0.4.7.11-1) ...
Setting up libc6-dev:amd64 (2.35-4) ...
Processing triggers for libc-bin (2.35-4) ...
Processing triggers for man-db (2.9.4-4) ...
Processing triggers for kali-menu (2021.4.2) ...
```

# install sshpass, a command line tool that will be used in our script to access remote server. This
# tool allow us to have non interactive access remote server in automated script by providing the
# password in the script.

sudo apt-get -qq install sshpass -y



```
Selecting previously unselected package sshpass.
(Reading database ... 289391 files and directories currently installed.)
Preparing to unpack .../sshpass_1.09-1+b1_amd64.deb ...
Unpacking sshpass (1.09-1+b1) ...
Setting up sshpass (1.09-1+b1) ...
Processing triggers for man-db (2.9.4-4) ...
Processing triggers for kali-menu (2021.4.2) ...
```

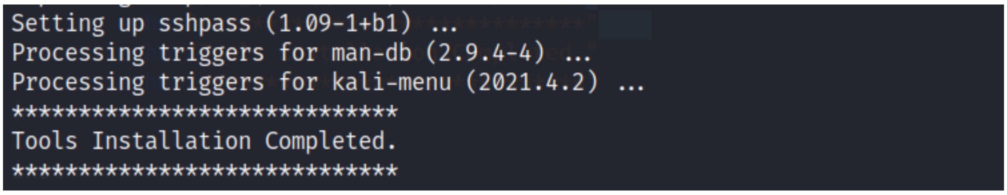
# Notify user that tool installation is completed, follow by an empty line for cosmetic reason.

*echo "*****************************"*

echo "Tools Installation Completed."

*echo "*****************************"*

}



```
Setting up sshpass (1.09-1+b1) ...
Processing triggers for man-db (2.9.4-4) ...
Processing triggers for kali-menu (2021.4.2) ...
*****************************
Tools Installation Completed.
*****************************
```

# inst is called to execute the inst function which comprises of the above codes.

inst

anon function

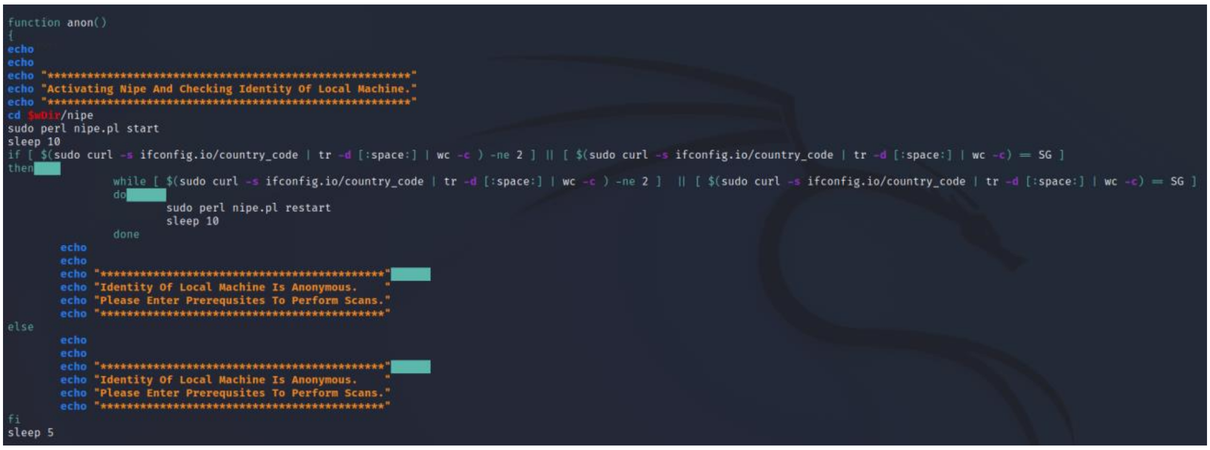
The anon function will execute the following actions:

1. Activate nipe (a script that uses Tor network our default gateway).
2. Access remote server via sshpass.
3. Scan target ip using remote server via sshpass.
4. Return scanned results to local machine.
5. Delete scanned results on remote server.

This section will break down the code to two parts for explanation.

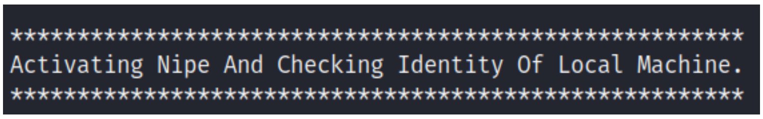
Nipe

A script that uses Tor network our default gateway. Once activated, this script routes our traffic from local machine to Tor network, which will make us anonymous. We can confirm our anonymity by checking our IP location on the internet.



```
function anon()
{
echo
echo
echo "********************************************************"
echo "Activating Nipe And Checking Identity Of Local Machine."
echo "********************************************************"
cd $wDir/nipe
sudo perl nipe.pl start
sleep 10
if [ $(sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c ) -ne 2 ] || [ $(sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c) == SG ]
then
                while [ $(sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c ) -ne 2 ]  || [ $(sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c) == SG ]
                do
                        sudo perl nipe.pl restart
                        sleep 10
                done
        echo
        echo
        echo "*******************************************"
        echo "Identity Of Local Machine Is Anonymous.    "
        echo "Please Enter Prerequsites To Perform Scans."
        echo "*******************************************"
else
        echo
        echo
        echo "*******************************************"
        echo "Identity Of Local Machine Is Anonymous.    "
        echo "Please Enter Prerequsites To Perform Scans."
        echo "*******************************************"
fi
sleep 5
```

```
# Start of anon function.
# Print out "Activating Nipe And Checking Identity Of Local Machine." To notify user of program
# status.
function anon()
{
echo
echo
echo "*******************************************************"
echo "Activating Nipe And Checking Identity Of Local Machine."
echo "*******************************************************"
```

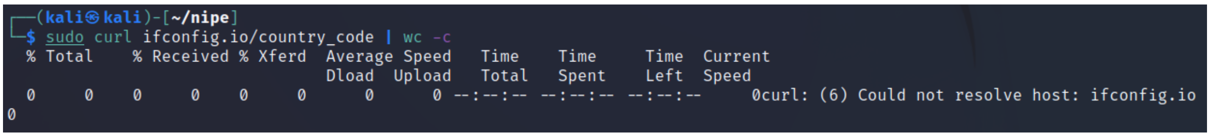


```
*******************************************************
Activating Nipe And Checking Identity Of Local Machine.
*******************************************************
```

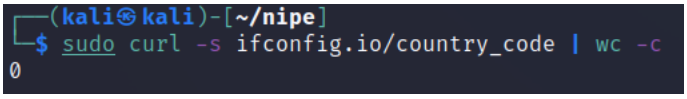
```
# cd into nipe folder
# Activate anonymity by sending a start command to the perl script 'nipe.pl'
# sleep 10, wait 10 seconds for nipe to be activated before proceed to next action
cd $wDir/nipe
sudo perl nipe.pl start
sleep 10
```

```
# start of if statement, when either condition are met, then a set of action will follow, breaking down
# the meaning of the condition.
# curl is a command line to transfer data, in this case retrieve data from 'ifconfig.io/country_code'
# -s command is to silent this operation
if [ $(sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c ) -ne 2 ]  ||
[ $(sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c) == SG ]
then
```

# Without -s flag a progress meter will be displayed, for this script -s flag will be included to mute the # progress meter.



```
┌──(kali㉿kali)-[~/nipe]
└─$ sudo curl ifconfig.io/country_code | wc -c
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0curl: (6) Could not resolve host: ifconfig.io
0
```



```
┌──(kali㉿kali)-[~/nipe]
└─$ sudo curl -s ifconfig.io/country_code | wc -c
0
```

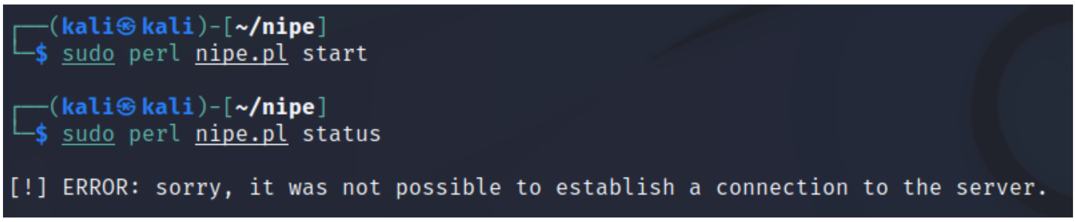
# tr -d [:space:] - to remove spaces from the retrieved data.

# wc -c - count the number of characters retrieved after removing the spaces.

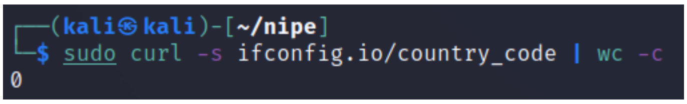
# -ne 2 – not equals to 2

# This condition will be met if the retrieved data, after removing spaces have more than or less than # 2 characters.

[$(sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c) -ne 2]



```
┌──(kali㉿kali)-[~/nipe]
└─$ sudo perl nipe.pl start

┌──(kali㉿kali)-[~/nipe]
└─$ sudo perl nipe.pl status

[!] ERROR: sorry, it was not possible to establish a connection to the server.
```



```
┌──(kali㉿kali)-[~/nipe]
└─$ sudo curl -s ifconfig.io/country_code | wc -c
0
```

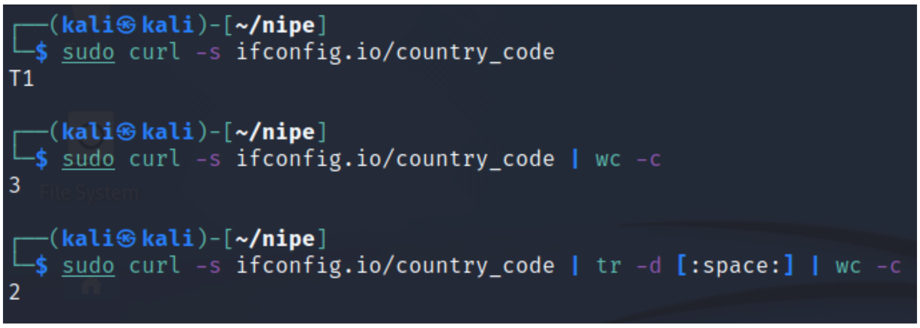
# Usually nipe is not able to start properly on the first try, it will output 0 characters. And a normal # country code should only have 2 characters.

# So, the if condition '-ne 2' is to ensure that when such error occur after starting nipe, the script is # able to automatically restart nipe until the error is rectified.

# This condition will be met if the retrieved data, after removing spaces is the characters 'SG'.

[$(sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c) == SG]

# The reason for adding ‘tr -d [:space:]’ command is to ensure the country code is displayed as 2
# characters, if not there will be an error in the if condition for country code equal ‘SG’.



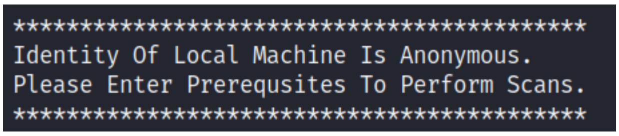
```
┌──(kali㉿kali)-[~/nipe]
└─$ sudo curl -s ifconfig.io/country_code
T1

┌──(kali㉿kali)-[~/nipe]
└─$ sudo curl -s ifconfig.io/country_code | wc -c
3

┌──(kali㉿kali)-[~/nipe]
└─$ sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c
2
```

# If either of the above conditions are met, a while loop will be executed, the conditions of while
# loop is the same as the above, checking either the retrieved data have more/less than 2 characters
# or is equals to ‘SG’. If this condition is met, then it will send a restart command to execute the
# nipe.pl script.

# Once the while loop confirms that neither of these conditions are true, meaning the retrieved date
# is exactly 2 characters and it is not ‘SG’, the script will exit the while loop and notify user that local
# machine’s identity is anonymous, input will be required to perform scans.

```
while [ $(sudo curl -s ifconfig.io/country_code | tr -d [:space:] | wc -c ) -ne 2 ]  || [ $(sudo curl -s
ifconfig.io/country_code | tr -d [:space:] | wc -c) == SG ]
                do
                        sudo perl nipe.pl restart
                        sleep 10
                done
        echo
        echo
        echo "*********************************************"
        echo "Identity Of Local Machine Is Anonymous.    "
        echo "Please Enter Prerequsites To Perform Scans."
        echo "*********************************************"
```

```
# When the 'If' statements confirms that neither of these conditions are true, meaning the retrieved
# date is exactly 2 characters and it is not 'SG', it will skip the while loop and notify user that local
# machine's identity is anonymous.

else

        echo

        echo

        echo "*******************************************"

        echo "Identity Of Local Machine Is Anonymous.    "

        echo "Please Enter Prerequsites To Perform Scans."

        echo "*******************************************"

fi

sleep 10
```



```
*******************************************
Identity Of Local Machine Is Anonymous.
Please Enter Prerequsites To Perform Scans.
*******************************************
```

Installing Tools on remote server and performing scan

# read -p flag means that the strings will be printed before reading an input from the terminal.

# ip variable stores ip address of remote server.

# username variable stores the username of remote server.

# password variable stores the password of remote server.

# targetip variable stores the ip address that we will be scan.

# port variable stores the ports that will be scan.

# filename variable stores the name that user want to save the scanned files as.

read -p "Enter the IP address of remote server: " ip

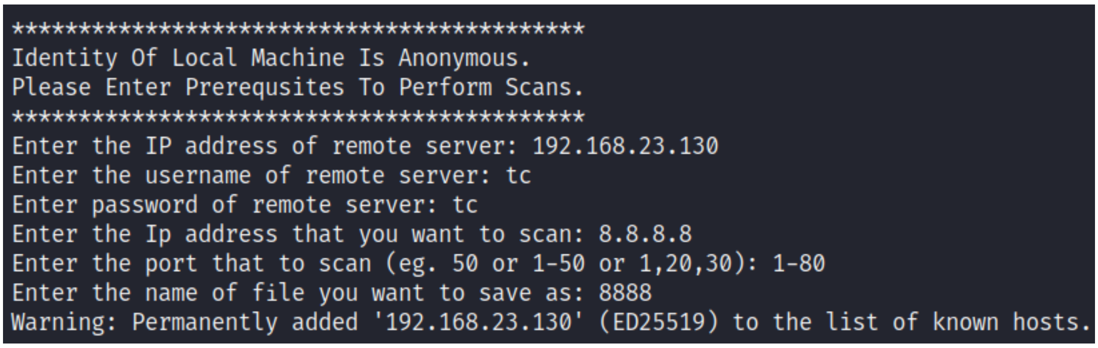
read -p "Enter the username of remote server: " username

read -p "Enter password of remote server: " password

read -p "Enter the Ip address that you want to scan: " targetip

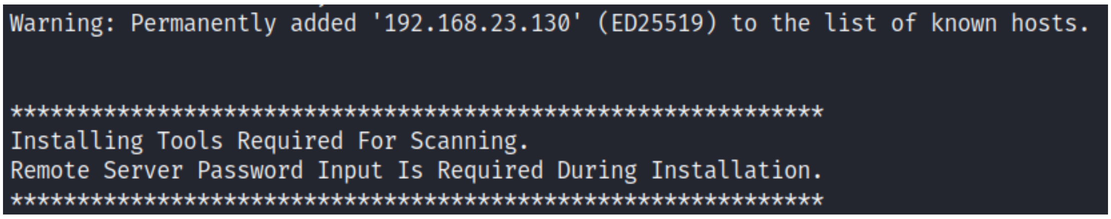
read -p "Enter the port that to scan (eg. 50 or 1-50 or 1,20,30): " port

read -p "Enter the name of file you want to save as: " filename



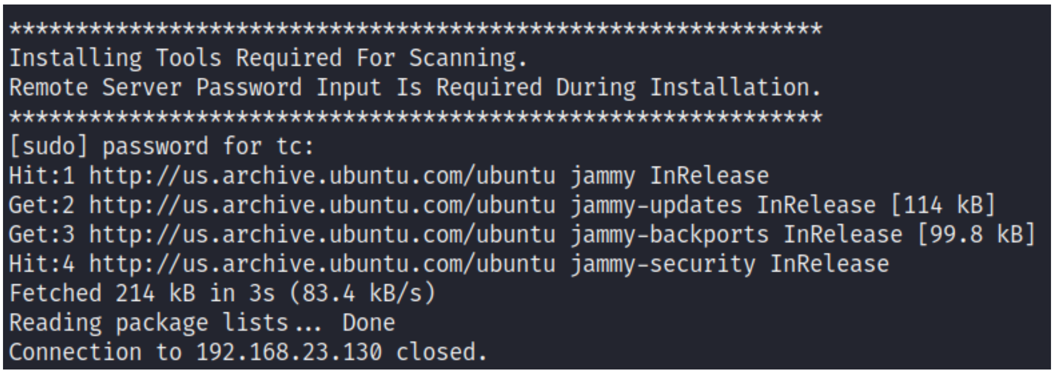
```
*******************************************
Identity Of Local Machine Is Anonymous.
Please Enter Prerequsites To Perform Scans.
*******************************************
Enter the IP address of remote server: 192.168.23.130
Enter the username of remote server: tc
Enter password of remote server: tc
Enter the Ip address that you want to scan: 8.8.8.8
Enter the port that to scan (eg. 50 or 1-50 or 1,20,30): 1-80
Enter the name of file you want to save as: 8888
Warning: Permanently added '192.168.23.130' (ED25519) to the list of known hosts.
```

```
# sshdir variable is use to store the path of remote server that we accessed, this path will be used
# later during secure copy to copy the scan results from remote server to local machine.

# -o StrictHostKeyChecking=no – add the remote server ip to local machine’s known host list so that
# ssh connection and authentication will not be rejected.

sshdir=$(sshpass -p $password ssh -o StrictHostKeyChecking=no $username@$ip "pwd")

echo

echo

echo "*************************************************************"

echo "Installing Tools Required For Scanning.                      "

echo "Remote Server Password Input Is Required During Installation."

echo "*************************************************************"

sleep 5
```

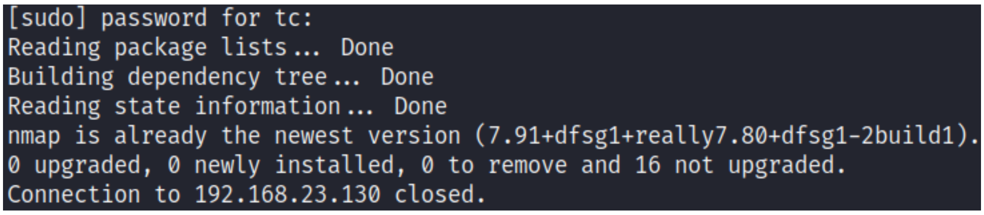


```
Warning: Permanently added '192.168.23.130' (ED25519) to the list of known hosts.


*************************************************************
Installing Tools Required For Scanning.
Remote Server Password Input Is Required During Installation.
*************************************************************
```

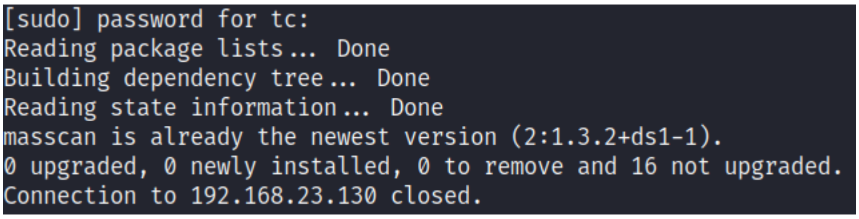
```
# -p – to input a password

# -t – force use of pseudo-terminal, if the command requires password input from remote server,
# the request will be printed on local machine waiting for input.

# The variables ‘password’, ‘username’, ‘ip’ are read from user input above.

# The command below connects local machine to remote server and execute the commands within
# the qutoes(“ ”) on remote server. These commands perform updates and tool installation on the
# remote server. The installed tools are nmap, masscan and whois.

# After tools installation are completed, it will notify user that tools installed and starting scan, then
# wait for 5 seconds before continuing to the next line of the script.

sshpass -p $password ssh -t $username@$ip “sudo apt-get update -y”

sshpass -p $password ssh -t $username@$ip “sudo apt-get install nmap -y”

sshpass -p $password ssh -t $username@$ip “sudo apt-get install masscan -y”

sshpass -p $password ssh -t $username@$ip “sudo apt-get install whois -y”

echo

echo

echo "***************"

echo "Tools Installed"

echo "***************"

sleep 5
```



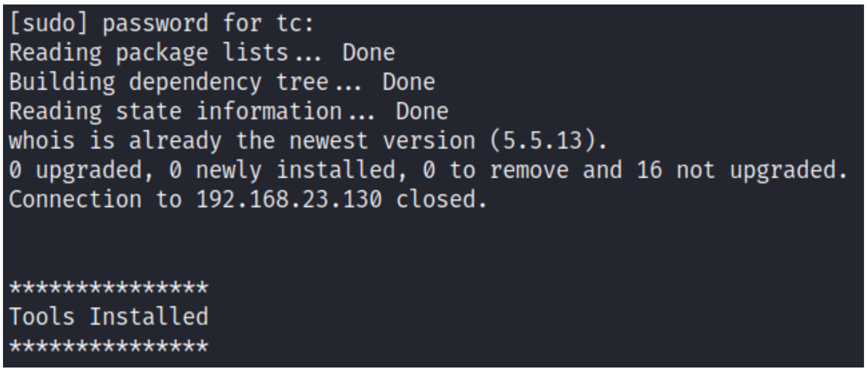
```
*************************************************************
Installing Tools Required For Scanning.
Remote Server Password Input Is Required During Installation.
*************************************************************
[sudo] password for tc:
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [99.8 kB]
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-security InRelease
Fetched 214 kB in 3s (83.4 kB/s)
Reading package lists... Done
Connection to 192.168.23.130 closed.
```



```
[sudo] password for tc:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2build1).
0 upgraded, 0 newly installed, 0 to remove and 16 not upgraded.
Connection to 192.168.23.130 closed.
```

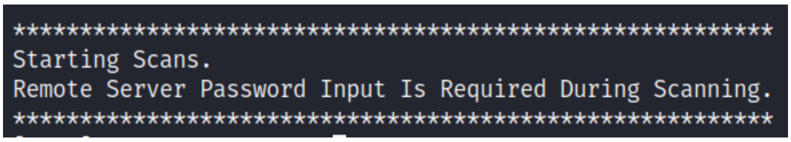


```
[sudo] password for tc:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
masscan is already the newest version (2:1.3.2+ds1-1).
0 upgraded, 0 newly installed, 0 to remove and 16 not upgraded.
Connection to 192.168.23.130 closed.
```



```
[sudo] password for tc:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
whois is already the newest version (5.5.13).
0 upgraded, 0 newly installed, 0 to remove and 16 not upgraded.
Connection to 192.168.23.130 closed.


***************
Tools Installed
***************
```

```
# Notify user scans are starting but some inputs are required for scanning, then wait for 5 seconds
# before continuing the next line of the script.

echo

echo

echo "*********************************************************"

echo "Starting Scans.                                          "

echo "Remote Server Password Input Is Required During Scanning."

echo "*********************************************************"

sleep 5
```



```
*********************************************************
Starting Scans.
Remote Server Password Input Is Required During Scanning.
*********************************************************
```

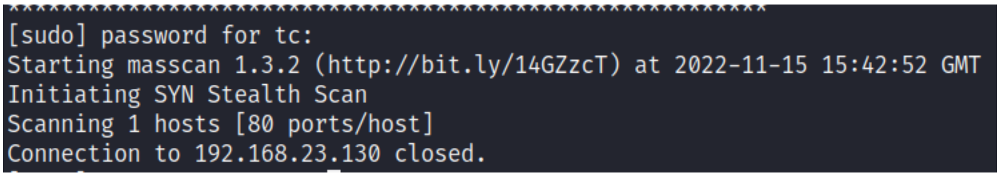
# This sshpass command connects local machine to remote server and uses the remote server to
# execute masscan the target. The variables ‘targetip’ , ‘port’ and ‘filename’ are retrieve from user
# input just before the tool installation on remote server.

# -open – scan for open ports only.

# -oG – save output format as 22grepable format, this flag is followed by the filename to save as.

# Other output formats can be use by changing -oG flag to oB(binary), oX (XML) or oJ(JSON).

sshpass -p $password ssh -t $username@$ip “sudo masscan $targetip -p$port –open -oG masscan$filename.grep”



```
*********************************************************
[sudo] password for tc:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-11-15 15:42:52 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [80 ports/host]
Connection to 192.168.23.130 closed.
```

# Observe sometimes that masscan scan result saved file is empty although the same command is
# being used. Tested direct on terminal, sometimes file contains result, sometimes it is empty.
# Conclude that the masscan is not as reliable as nmap.

# This sshpass command connects local machine to remote server and uses the remote server to
# execute nmap the target, then followed by wait 5 seconds before proceed to next line of the script.

# -sV – check service and version info from open ports.

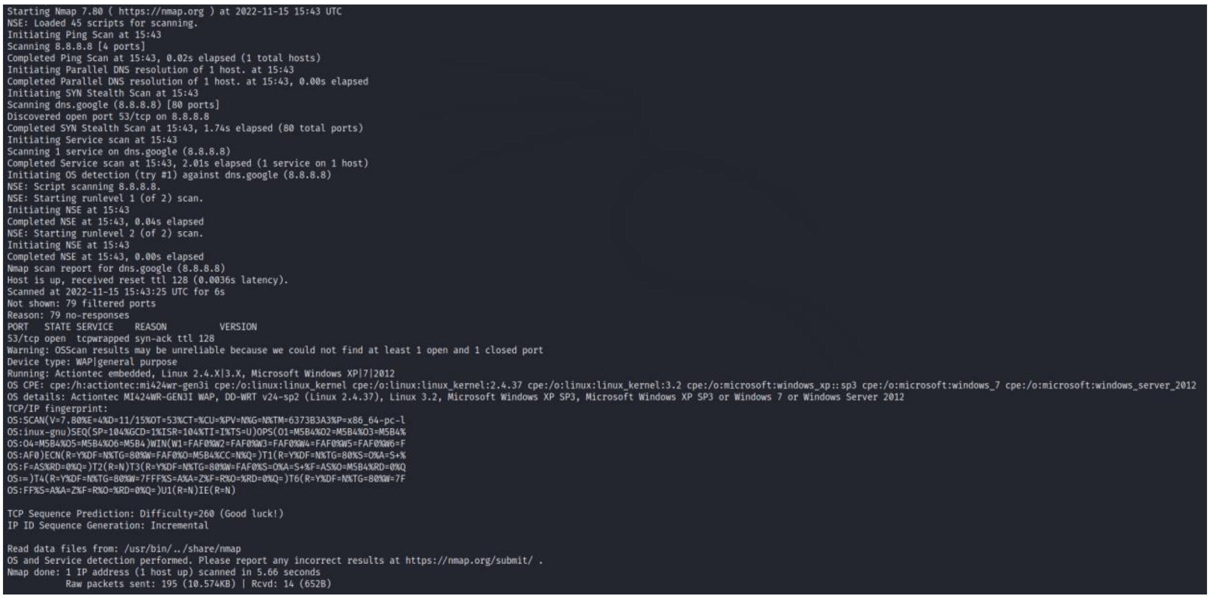
# -O – Detect the Operating System target is using.

# -vv – increase verbosity level, useful for troubleshoot if errors encountered during scanning.

# -oA – save all output formats(normal, xml , grepable), this flag is followed by the filename to save
as.

sshpass -p $password ssh -t $username@$ip "sudo nmap $targetip -p$port -sV -O -vv -oA $filename"

sleep 5



```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-15 15:43 UTC
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 15:43
Scanning 8.8.8.8 [4 ports]
Completed Ping Scan at 15:43, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:43
Completed Parallel DNS resolution of 1 host. at 15:43, 0.00s elapsed
Initiating SYN Stealth Scan at 15:43
Scanning dns.google (8.8.8.8) [80 ports]
Discovered open port 53/tcp on 8.8.8.8
Completed SYN Stealth Scan at 15:43, 1.74s elapsed (80 total ports)
Initiating Service scan at 15:43
Scanning 1 service on dns.google (8.8.8.8)
Completed Service scan at 15:43, 2.01s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against dns.google (8.8.8.8)
NSE: Script scanning 8.8.8.8.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:43
Completed NSE at 15:43, 0.04s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Nmap scan report for dns.google (8.8.8.8)
Host is up, received reset ttl 128 (0.0036s latency).
Scanned at 2022-11-15 15:43:25 UTC for 6s
Not shown: 79 filtered ports
Reason: 79 no-responses
PORT   STATE SERVICE    REASON          VERSION
53/tcp open  tcpwrapped syn-ack ttl 128
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=11/15%OT=53%CT=%CU=%PV=N%G=N%TM=6373B3A3%P=x86_64-pc-l
OS:inux-gnu)SEQ(SP=104%GCD=1%ISR=104%TI=I%TS=U)OPS(O1=M5B4%O2=M5B4%O3=M5B4%
OS:O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=FAF0%W2=FAF0%W3=FAF0%W4=FAF0%W5=FAF0%W6=F
OS:AF0)ECN(R=Y%DF=N%TG=80%W=FAF0%O=M5B4%CC=N%Q=)T1(R=Y%DF=N%TG=80%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=N%TG=80%W=FAF0%S=O%A=S+%F=AS%O=M5B4%RD=0%Q
OS:=)T4(R=Y%DF=N%TG=80%W=7FFF%S=A%A=Z%F=R%O=%RD=0%Q=)T6(R=Y%DF=N%TG=80%W=7F
OS:FF%S=A%A=Z%F=R%O=%RD=0%Q=)U1(R=N)IE(R=N)

TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.66 seconds
           Raw packets sent: 195 (10.574KB) | Rcvd: 14 (652B)
```

# This sshpass command connects local machine to remote server and uses the remote server to
# execute whois on the target.

# After whois is perform on target, the data is saved to a file named ‘whois<filename defined by
# user>’.

# Notify user that scanning is completed.

sshpass -p $password ssh $username@$ip "whois $targetip > whois$filename"

echo "******************************"

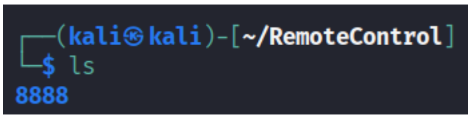
echo "Scanning On Target Completed."

# cd into RemoteControl directory

# Create a new folder on local machine with the file name defined by user to store the scanned
# results.

cd $wDir/RemoteControl

mkdir $filename



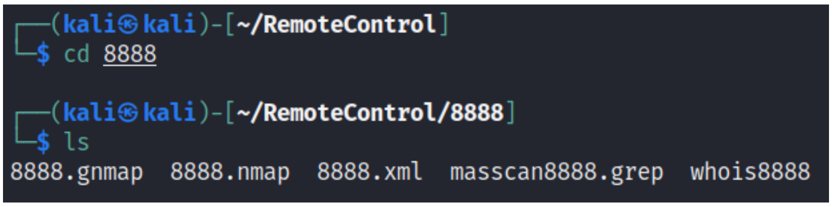
```
┌──(kali㉿kali)-[~/RemoteControl]
└─$ ls
8888
```

# Execute a secure copy via sshpass from remote server.

# Copy all files with filename defined by user from the path where we access and save the scan
# results.

# Copy to the folder created on local machine.

sshpass -p $password scp $username@$ip:$sshdir/*$filename ./$filename*

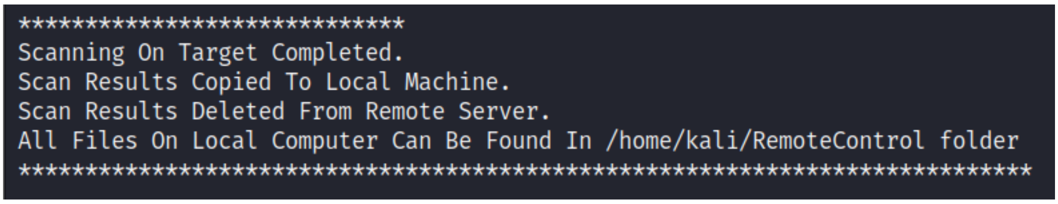


```
┌──(kali㉿kali)-[~/RemoteControl]
└─$ cd 8888

┌──(kali㉿kali)-[~/RemoteControl/8888]
└─$ ls
8888.gnmap  8888.nmap  8888.xml  masscan8888.grep  whois8888
```

# notify user that scan results are copied to local machine.

echo "Scan results copied to local machine."

```
# Access and delete all scan results on remote server, then notify user all scan results deleted from
# remote server.

# Lastly notify user the path in local machine where scan results in stored.

sshpass -p $password ssh -o StrictHostKeyChecking=no $username@$ip "rm -r $sshdir/*$filename*"

echo "Scan Results Deleted From Remote Server."

echo "All Files On Local Computer Can Be Found In $wDir/RemoteControl folder"

echo "****************************************************************************"

}
```



```
*****************************
Scanning On Target Completed.
Scan Results Copied To Local Machine.
Scan Results Deleted From Remote Server.
All Files On Local Computer Can Be Found In /home/kali/RemoteControl folder
****************************************************************************
```

```
# This is to call the 'anon' function for execution.

anon
```

Reference

NIPE -- Fully Anonymize Total Kali Linux System

https://www.kalilinux.in/2022/02/total-anonymous-kali-linux.html

How to put sshpass command inside a bash script?

https://exchangetuts.com/how-to-put-sshpass-command-inside-a-bash-script-1640250664982761

sudo over ssh: no tty present and no askpass program specified

https://unix.stackexchange.com/questions/48554/sudo-over-ssh-no-tty-present-and-no-askpass-program-specified

Bash Scripting – If Statement

https://www.geeksforgeeks.org/bash-scripting-if-statement/

How to Install Nipe tool in Kali Linux?

https://www.geeksforgeeks.org/how-to-install-nipe-tool-in-kali-linux/

End