

Summary

মঙ্গলবার, 6 জুলাই, 2021 2:56 AM

Goal: Connect to bandit.labs.overthewire.org on port: 2220 ; username: bandit0 ; password: bandit0

Procedure: used `ssh <hostname>@<remote/web name> -p port_number` command to connect

Result: Successful connection

SSH checking

মঙ্গলবার, 6 জুলাই, 2021 2:57 AM

Ssh was installed. Checked by the command ssh

\$ssh

usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
[-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
[-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
[-i identity_file] [-J [user@]host[:port]] [-L address]
[-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
[-Q query_option] [-R address] [-S ctl_path] [-W host:port]
[-w local_tun[:remote_tun]] destination [command]

SSH Connection

মঙ্গলবার, 6 জুলাই, 2021 3:09 AM

Used `ssh <hostname>@<remote/web name> -p port_number` command to connect to the bandit server at 2220 port through ssh.

```
-(manarat@kali)-[~]
```

```
└─$ ssh bandit0@bandit.labs.overthewire.org -p 2220
```

The authenticity of host '[bandit.labs.overthewire.org]:2220 ([176.9.9.172]:2220)' can't be established.

ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X3OPnyPSB5tB5RPbhczc.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[176.9.9.172]:2220' (ECDSA) to the list of known hosts.

This is a OverTheWire game server. More information on <http://www.overthewire.org/wargames>

bandit0@bandit.labs.overthewire.org's password:

Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

```

      ,--..      ,--..      ,--..
    /  / \      /  / \      /  / \
   / . . :  / . . :  / . . :
  . / ; \ ; ; / / _ \ \ ; |
 . ; / ` ; ' _ _ / ' . . ' \ .
 ; | ; \ ; | | : | / _ \ \ | ''
 | : | ; | ' ; | ; ; \ \ \ :
 . | ' ' : ' _ _ | | \ ; ` |
 ' ; \ / | ' : ; . \ \ \ ;
 \ \ ' / | | ' | ' \ \ \ \ |
 ; : / ' : | : ' | --"
 \ \ ' ; | ' \ \ \
www. `---` ver `---` he `---` ire.org

```

Welcome to OverTheWire!

If you find any problems, please report them to Steven or morla on irc.overthewire.org.

--[Playing the games]--

This machine might hold several wargames.

If you are playing "somegame", then:

* USERNAMES are somegame0, somegame1, ...

- * Most LEVELS are stored in /somegame/.
- * PASSWORDS for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled so that users can not snoop on eachother. Files and directories with easily guessable or short names will be periodically deleted!

Please play nice:

- * don't leave orphan processes running
- * don't leave exploit-files laying around
- * don't annoy other players
- * don't post passwords or spoilers
- * again, DONT POST SPOILERS!

This includes writeups of your solution on your blog or website!

--[Tips]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

```
-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,norelro    disable relro
```

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[Tools]--

For your convenience we have installed a few usefull tools which you can find in the following locations:

- * gef (<https://github.com/hugsy/gef>) in /usr/local/gef/
- * pwndbg (<https://github.com/pwndbg/pwndbg>) in /usr/local/pwndbg/
- * peda (<https://github.com/longld/peda.git>) in /usr/local/peda/
- * gdbinit (<https://github.com/gdbinit/Gdbinit>) in /usr/local/gdbinit/
- * pwntools (<https://github.com/Gallopsled/pwntools>)
- * radare2 (<http://www.radare.org/>)

* checksec.sh (<http://www.trapkit.de/tools/checksec.html>) in /usr/local/bin/checksec.sh

--[More information]--

For more information regarding individual wargames, visit

<http://www.overthewire.org/wargames/>

For support, questions or comments, contact us through IRC on

irc.overthewire.org #wargames.

Enjoy your stay