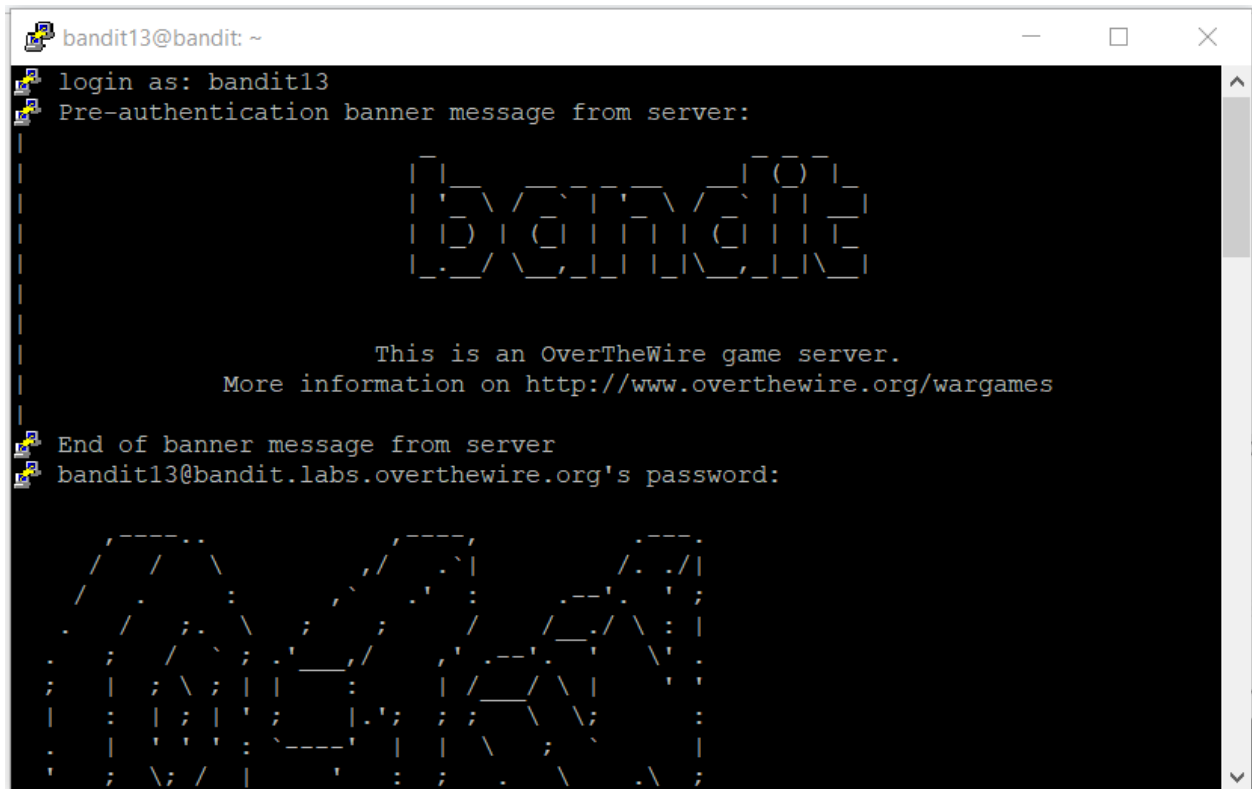


Bandit OTW Walkthrough Write-Up

Level : 13 → 14

Challenge: The password for the next level is stored in `/etc/bandit_pass/bandit14` and can only be read by user `bandit14`. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. Note: `localhost` is a hostname that refers to the machine you are working on

Step 1: Make sure you used the password from the previous level (Level 12 → 13) to login to `bandit13`.



```
bandit13@bandit: ~
login as: bandit13
Pre-authentication banner message from server:

      OverTheWire

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

End of banner message from server
bandit13@bandit.labs.overthewire.org's password:
```

Step 2:

```
bandit13@bandit: ~  
bandit13@bandit:~$ pwd  
/home/bandit13  
bandit13@bandit:~$ ls  
sshkey.private  
bandit13@bandit:~$ cat sshkey.private  
-----BEGIN RSA PRIVATE KEY-----  
MIIEpAIBAACAQEAxkkoE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+  
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AioYp0MZYETq46t+jk9puNwZwIt9XgB  
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb  
ThMsiMnyJafEwJ/T8PQO3myS91vUHEuoOMAZoUID4kN0MEZ3+XahyK0HJVq68KsV  
ObefXG1vvA3GAJ29kxJaqrVfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0Snxana+WYA7  
jiPyTF0is8uzMlYQ411Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA  
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+bBw3RXvzE  
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjjNAqx/TLfz1LYfOu7i9Jet67  
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS  
nXmwYckKUcUgzoVSpINzaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYcktsD  
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONTmrVvtYK40/yeU4aZ/HA2DQzwhe  
ollAfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhpNTDUy5WGrpScRXomsVIBUf  
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS  
M1F2fstxVqPtZDlDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNh3McdURjAoGBANKU  
lhqfnw7+aXncJ9bjysrlZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH  
PKWkJNDBG+ex0H9JNQsTK3X5PBMA8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s  
8DtVCxDuVsM+i4X8UqIGOlvgbtKEVokHPFXPlq/dAoGAcHg5YX7WEehCgCYTzpO+  
xysX8ScM2qS6xuZ3MqUWaxUWkh7NGZvhe0sGy9iOdANzWk7mUUFViacMR/t54W1
```

```
bandit13@bandit: ~  
ObefXG1vvA3GAJ29kxJaqrVfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0Snxana+WYA7  
jiPyTF0is8uzMlYQ411Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA  
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+bBw3RXvzE  
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjjNAqx/TLfz1LYfOu7i9Jet67  
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS  
nXmwYckKUcUgzoVSpINzaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYcktsD  
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONTmrVvtYK40/yeU4aZ/HA2DQzwhe  
ollAfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhpNTDUy5WGrpScRXomsVIBUf  
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS  
M1F2fstxVqPtZDlDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNh3McdURjAoGBANKU  
lhqfnw7+aXncJ9bjysrlZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH  
PKWkJNDBG+ex0H9JNQsTK3X5PBMA8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s  
8DtVCxDuVsM+i4X8UqIGOlvgbtKEVokHPFXPlq/dAoGAcHg5YX7WEehCgCYTzpO+  
xysX8ScM2qS6xuZ3MqUWaxUWkh7NGZvhe0sGy9iOdANzWk7mUUFViacMR/t54W1  
GC83sOs3D7n5Mj8x3Nd08xFit7dT9a245TvaoYQ7KgmqpsG/ScKCw4c3eiLava+J  
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY  
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ519JmEsBh7SadkwsZhvecQcS9t4vby  
9/8X4jS0P8ibfcsK4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsq+w32xeD  
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0  
kAWpXbv5tbkkzbs0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN  
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==  
-----END RSA PRIVATE KEY-----  
bandit13@bandit:~$ man ssh  
bandit13@bandit:~$
```

```
bandit13@bandit: ~  
with a PKCS#11 token providing keys for user authentication.  
  
-i identity file  
Selects a file from which the identity (private key) for public  
key authentication is read. You can also specify a public key  
file to use the corresponding private key that is loaded in  
ssh-agent(1) when the private key file is not present locally.  
The default is ~/.ssh/id_rsa, ~/.ssh/id_ecdsa,  
~/.ssh/id_ecdsa_sk, ~/.ssh/id_ed25519, ~/.ssh/id_ed25519_sk and  
~/.ssh/id_dsa. Identity files may also be specified on a per-  
host basis in the configuration file. It is possible to have  
multiple -i options (and multiple identities specified in config  
uration files). If no certificates have been explicitly speci  
fied by the CertificateFile directive, ssh will also try to load  
certificate information from the filename obtained by appending  
-cert.pub to identity filenames.  
  
-J destination  
Connect to the target host by first making a ssh connection to  
the jump host described by destination and then establishing a  
TCP forwarding to the ultimate destination from there. Multiple  
jump hops may be specified separated by comma characters. This  
is a shortcut to specify a ProxyJump configuration directive.  
Manual page ssh(1) line 139 (press h for help or q to quit)
```

```
bandit14@bandit: ~  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit14@bandit:~$ ls  
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14  
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq  
bandit14@bandit:~$
```

fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

Privatekeylevel13.txt - Notepad

File Edit Format View Help

-----BEGIN RSA PRIVATE KEY-----

```
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IwhFc9aPaaQmQDdgzuXcv+ppZHa++buSkN+
gg0Tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwbFw/vVLNwOXBe4UwStGRWzgpPeeSv5Tb1VjLZIBdgphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQ03mys91vUHEuo0MAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29KxJaqvRfgYnqZryWn7w3CHjNU4c/2Jkp+n8L0SnxaNA+wYA7
jiPyTF0is8uzM1YQ411Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dwBjhYEozjeA
J3j/Rwmap9MSzfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfyoAQSS+bBw3RXvze
pvJt3SmU8hIDuLscJL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfz1LYfOu7i9Jte67
xAh0tONG/u8FB5I3LAI2Vp6OviwvdeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUCugzoVSpINzaS0zUDypdp2+trH3MQa5kqN1YKjvF8RC47woOYCKtsD
o3FPpGNFec9Taa3Msy+DfQqHhKZFKIL3bJDOntmrVvtYK40/yeU4aZ/HA2DQzWhe
o11AfIEhAoGBAOnVjosBkm7sb1k+n4IEwPxs8s0mhPntDUy5WGrpScRX0msVIBUF
1aL3ZGLx3xCiwtCnEucB9DvN2HZkucp/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxvqPtZDlDmwjNR04XHA/fkh8bXXyTMqOHnJTHHNhbb3McdURjAoGBANku
1hqfnw7+aXncJ9bjysr1ZwbQOE5Nd8AFgfwaKuGTTVX2NsUQnCMmdop+wFak40JH
PKWkJndBG+ex0H9JNqsTK3X5PBMA58AfX0GrKeuwKwA6erytVTqjOfLYcdp5+z9s
8DtVCXduVsM+i4X8UqIGo1vgbtKEVokHPFXP1q/dAoGACHg5YX7WEehCgCYTzpO+
xys8S8cM2Qs6xuZ3MqUWAXUwkh7NGZvhe0Sgy9iOdANzwKw7mUUFVIAcMR/t54W1
GC83s0s3D7n5Mj8x3Nd08xFit7dT9a245Tva0YQ7KgmpqSg/ScKcW43eiLava+J
3bttJesIU+8ZX9XjPrPkwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNPbY
idkyZ8ySF8G1cFsky8Yw6fWcQf63zDrohJ519jmEsBh7SadkwsZhvecQcS9t4vby
9/8X4js0P8ibfCKS4nBP+dT81kkkg5Z5MohXBORA7Vwx+AcOhcDEkprsqw32xeD
qt1EvQKbgQK8ws2ByvSUVs9GjTilCajFqLJ0eVvZRpAY6f+Gv/UVFAPV4c+S0
kAWpXbv5tbkzbs0eaLPTKGLzavXtQoTtKwrjpolHKIHuz6wu+n4abfAIRFubodN
/+aLoR0yBDRbdXMsZn/jvY44eM+xRLdRVyMmdPtP8be1Ri2E2aEZA=
-----END RSA PRIVATE KEY-----
```



PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDAQDGSQ4TzdbZw5PshaEVz1o9ppCZAN2D05cK/6mlkdr75u5KQ36CDS1yvsXD
w0sZrn5TN5zasSDRaZ568HXcAihinQxnIROrjq360T2m43BnAi31eAFm58a1kTBZsVbD+9Us3A5cF7hRZK0ZFbOA
+kR5Kj/INvVWMtkgF0amFMgrbYCbPpItOEyyilyflp8TAn9Pw9A7ebJL3W9QcS6g4wDOhQgPiQ3QwRnf5dqHlrQclWrrwqxU
5t59cbW+8DcYAnb2TElq9F+BiepmvJY3vDcleM1Thz/YmSn6fwvRKf0o0D5ZgDuOI/JMXSKzy7MyVhDiXUvOH/z8ym
```

Key fingerprint: ssh-rsa 2048 SHA256:51TWBGKdiJZHVGOnADWzflLdsmqExtqBKuHflyODtig

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Generate

Load an existing private key file

Load

Save the generated key

Save public key

Save private key

Parameters

Type of key to generate:

☒ RSA

☐ DSA

☐ ECDSA

☐ EdDSA

☐ SSH-1 (RSA)

Number of bits in a generated key:

2048