

OverTheWire: Bandit

Riley Fleming
Penetration Testing
Professor Beco
May 16, 2022



Introduction

OverTheWire: Bandit

- **Wargame**
- For **beginners**
- Teaches the **basics**
- **Level based**



Table of Contents



Level 12

command list

grep, sort, uniq, strings, base64, tr, tar,
gzip, bzip2, xxd, mkdir, cp, mv, file

Level 24

command list

cd, mkdir, nano, touch, echo, cat, chmod

Level 23

command list

cron, crontab, cd, cat, mkdir, nano,
chmod, touch

Level 29

command list

git, mkdir, cd, cat



Level 12

Level Goal: Uncompress the hexdump file (**data.txt**) we have been given. Number of compressions is unknown.

- Make temporary directory, copy **data.txt** to temporary directory
- cat **data.txt**, confirming it is a hexdump
- Use **xxd -r data.txt > data1**
- Check file type using **file data1**
- Change file extension with **mv data1 data.(gz,bz2, tar)**
- Unzip file (Ex. **gunzip, bunzip2, tar -xvf**)
- Repeat process 8 times
- Once the **ASCII** file is reached, **cat** file and obtain password

bzip2




Level 23



```
iLE88D} :{088888D};  
:LGtE888D, f8Gj}jLE888E;  
iE :8888Et. :G8888;  
:1 E888, :8888;  
D888, :8888;  
D888, :8888;  
D888, :8888;  
D888, :8888;  
888W, :8888;  
W88W, :8888;  
W88W, :8888;  
DGGD: :8888;  
:8888;  
:W888;  
:8888;  
E8881  
tW88D
```

Level Goal: Determine how to take advantage of a cronjob.

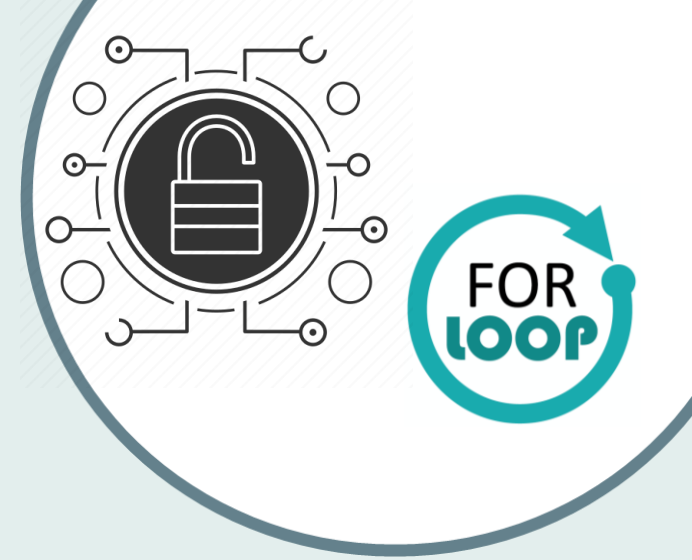
- Maneuver to **/etc/cron.d**
- Find configuration file **cronjob_bandit24**. (**ls**, **cat**)
- Job executed every minute
- Change directory to **/usr/bin**
- **cat cronjob_bandit24.sh** (shell script)
- Script executes and deletes all scripts located in **/var/spool**
- Create script ----->
- **chmod 777** (script, redirect file, and directory)
- **cp** script to **/var/spool**
- **cat givemepass123**



```
#!/bin/bash  
cat  
/etc/bandit_pass/bandit24 >  
/tmp/windr/givemepass123
```

Level 24

Level Goal: Find a way to obtain secret 4-digit pin and the next level's password. HINT: brute force.



- Make temporary directory
- Create script ----->
- **chmod 777 windscript.sh**
- **./windscript.sh**

```
#!/bin/bash
touch passwordchecker.txt
for i in {0000..9999}
do
    echo "UoMYTrfrBFHyQXmg6gzctqAwOmw1lohZ $i"
done | nc localhost 30002 > passwordchecker.txt

cat passwordchecker.txt | grep -v Wrong)
```





Level 29

Level Goal: There is a git repository at `ssh://bandit29-git@localhost/home/bandit29-git/repo`. The password for the user `bandit29-git` is the same as for the user `bandit29`.



- Make temporary directory
- Clone git repo (**`git clone ssh://bandit29-git@localhost/home/bandit29-git/repo`**)
- cd into **repo**
- **cat README.md** (no password)
- Check logs (**`git log`**) (no changes)
- Check other branches (**`git branch -r`**)
- Swap to dev branch (**`git checkout dev`**)
- Check logs again
- Revert to old commit (**`git checkout "old commit"`**)
- **cat README.md**

OverTheWire: Bandit

By: Riley Fleming

