SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Information Systems Security Audit & Control

4th Year 2nd Semester 2016

Name: Harshanath W.W.D.K

SLIIT ID: IT13069032

Practical Session: WE Friday

Practical Number: Lab 2

Date of Evaluation : ________________________

Evaluators Signature : ________________________

Wargames by OverTheWire

In hacking, a wargame (or war game) is a cyber-security challenge and mind sport in which the competitors must exploit or defend a vulnerability in a system or application, or gain or prevent access to a computer system.

A wargame usually involves a capture the flag logic, based on penetration test, semantic URL attacks, knowledge-based authentication, password cracking, reverse engineering of software (mostly JavaScript, Adobe Flash, and assembly language), code injection, SQL injections, cross-site scripting, exploits, IP address spoofing, and other hacking techniques.

Bandit

The Bandit wargame is aimed at absolute beginners. It will teach the basics needed to be able to play other wargames. This game, like most other games, is organized in levels. You start at Level 0 and try to “beat” or “finish” it. Finishing a level results in information on how to start the next level. The pages on this website for “Level <X>” contain information on how to start level X from the previous level.

MobaXterm

MobaXterm is your ultimate toolbox for remote computing. In a single Windows application, it provides loads of functions that are tailored for programmers, webmasters, IT administrators and pretty much all users who need to handle their remote jobs in a simpler fashion.

We have to log into the game using SSH. The host to which we need to connect is bandit.labs.overthewire.org. MobaXterm is used to connect to the corresponding server. We can also use the Putty SSH client for the same purpose.

Level 0

```
cat readme
```

```
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
```

Level 1

```
cat < -
```

```
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
```

Level 2

```
cat < spaces\ in\ this\ filename
```

```
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

Level 3

```
ls -a cat .hidden
```

```
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

Level 4

```
cat < -file07
```

```
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
```

Level 5

```
find -readable -size 1033c ! -executable //1333c(c for actual bytes) f type (file) size (sizein actual bytes) not executable(!)
```

```
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Level 6

```
find / -user bandit7 -group bandit6 -size 33c 2>&1| grep -v "Permission denied" find (user) (group) (size) (stdout to std in)
```

```
pwd :/var/lib/dpkg/info
```

```
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

Level 7

```
grep millionth data.txt
cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

Level 8

```
sort data.txt |uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
```

Level 9

```
strings data.txt | grep "="
truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
```

Level 10

```
base64 --decode data.txt
IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
```

Level 11

```
sort data.txt | tr '[a-zA-Z]' '[n-za-mN-ZA-M]'
5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

Level 12

```
bzip2 -d data6.bin.gz2
file data6.bin.out
tar -xvf data6.bin.out
file data8.bin
zcat -d data8.bin > data9.bin
file data9.bin
cat data9.bin
8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
```

Level 13

```
ssh -i sshkey.private bandit14@localhost cat /etc/bandit_pass/bandit14
```

```
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
```

Level 14

using net cat `echo 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e | nc -v localhost 30000`

```
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

Level 15

```
echo BfMYroe26WYalil77FoDi9qh59eK5xNr | openssl s_client -quiet -connect localhost:30001
```

```
cluFn7wTiGryunymYOu4RcffSxQluehd
```