htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

Ethical hacking of a CTF-VM

Laboratory protocol Exercise 7: Ethical hacking of a CTF-VM

Figure 1: Grouplogo

Subject: ITSI
Class: 3AHITN
Name: Stefan Fürst, Justin Tremurici
Groupname/number Name here/12
Supervisor: SPAC, ZIVK
Exercise dates:
Submission date:

htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

Contents

1 Task definition **3**

2 Summary **3**

3 Complete network topology of the exercise **4**

4 Exercise Execution **5**
4.1 Setting up the Virtual mascheines . . . 5
4.2 scanning the network . . . 5
4.3 exploring the websites . . . 5
4.4 breaking the http authtication . . . 5
4.5 sshing into the server . . . 5
4.6 exploring the system . . . 5
4.7 procces flag . . . 5
4.8 comment flag . . . 5
4.9 sudo flag . . . 5
4.10 history flag . . . 5
4.11 tmp flag . . . 5
4.12 it's over but actually not . . . 5
4.13 trying to escalate privaledgs . . . 5
4.13.1 smart enumeration . . . 5
4.13.2 trying a kernel level exploit . . . 5
4.13.3 checking suid binarys . . . 5
4.13.4 checking root proccses . . . 5
4.13.5 trying metasploit . . . 5
4.13.6 trying other common ctf priv escalation ways . . . 5
4.14 reseting the root password and exploring the vm . . . 5
4.15 7 flags . . . 5
4.16 talking abt the setup etc or sum idk :shruge: . . . 5

5 References **6**

6 List of figures **7**

1 Task definition

2 Summary

3 Complete network topology of the exercise

4 Exercise Execution

4.1 Setting up the Virtual mascheines

4.2 scanning the network

4.3 exploring the websites

4.4 breaking the http authtication

4.5 sshing into the server

4.6 exploring the system

4.7 procces flag

4.8 comment flag

4.9 sudo flag

4.10 history flag

4.11 tmp flag

4.12 it's over but actually not

4.13 trying to escalate privaledgs

4.13.1 smart enumeration

4.13.2 trying a kernel level exploit

4.13.3 checking suid binarys

4.13.4 checking root proccses

4.13.5 trying metasploit

4.13.6 trying other common ctf priv escalation ways

4.14 reseting the root password and exploring the vm

4.15 7 flags

4.16 talking abt the setup etc or sum idk :shruge:

5 References

References

6 List of figures

List of Figures

1 Grouplogo 1