Exercise 12 Penetration Test Report

Nipuna Weerasinghe

11 October 2017

Contents

Executive Summary

We were contracted by M3g4C0rp in order to use PowerUp to identify any misconfigurations on the HERD machine.

We were able to mount the PowerUp file and import the module to identify the password of the Local Administrator account.

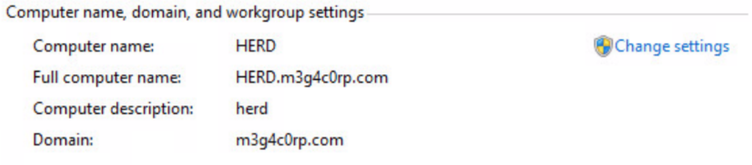
Recommendation Summary

In order to make sure that this misconfiguration is not further exploited in the future, make sure that Remote Desktop Service is disabled in the settings of the machine.

Technical Report

Information Gathering

It was possible to know that the remote machine was herd through the System information in the Control Panel.



Computer name, domain, and workgroup settings

Computer name: HERD

Full computer name: HERD.m3g4c0rp.com

Computer description: herd

Domain: m3g4c0rp.com

We mounted the PowerUp file path and logged into the remote machine as per Exercise 11:

rdesktop -r disk:win32=/usr/share/PowerSploit 172.30.0.3

Vulnerability Assessment

Technical Vulnerabilities

Once logged into the machine, we were able to navigate to the mounted file path using the File Explorer. We then opened up a command prompt and typed the following in order to get a Powershell window with bypassed execution.

powershell -exec bypass

We then imported the PowerUp module using the following command. *Import-Module ..ps1*

Once the module was imported successfully, we then ran the command to identify all the misconfigurations.

Invoke-AllChecks

This command then helped us identify the password for the LocalAdmin Account.

W3 is a great minister

Summary of Results

Exploitation/Vulnerability Confirmation

Exploitation Timeine

Target was exploited within 1 hour.

Targets Selected for Exploitation

herd.m3g4c0rp.com
S.Shephard and LocalAdmin accounts.

Directed Attack Used the PowerUp Module in order to get the password of the LocalAdmin Account.

Target Hosts Able to be Exploited LocalAdmin account on herd.m3g4c0rp.com

Attacks conducted PowerUp exploit to gain Admin Password.

Attacks Successful Above attack was successfull.

Level of Access Granted +Escalation Path Full Administration privellages were granted to herd.m3g4c0rp.com.

Remediation Disable Remote desktop service so that attacks like these are not possible in the future.

Post-Exploitation

Privilege Escalation Path

Technique Used
Used the PowerUp Module and PowerSploit method in order to get access to the password of the LocalAdmin Account.

Acquisition of Critical Information Defined by Client

Was able to access group privileges and other files on the system.

Conclusion

This was a successful attempt in exploiting the common misconfiguration of using the Remote Desktop Service to access a system. We utilised the PowerSploit technique and PowerUp module to get the password of the Local Administrator account which is a very severe breach in the system.