CS 615

Assignment 4: Service Enumeration & Cracking

PART 1: Service Enumeration

In the tasks below write the commands have you used with options

1. List all the services running on Metasploitable machine and provide a short description (5 lines maximum) for each service.

2. List all the services running on Windows Server machine and provide a short description for each service.

3. Find the ssh service on Metasploitable machine in the port range 700-1000

4. Find any service running UDP on Windows Server machine.

5. Try to brute force the FTP service running on Metasploitable machine

6. Using the FTP service running on Metasploitable machine, create a directory called a XD and create the file xd.txt of that directory.

PART 2: Tools

For (1-3) , follow the steps using your own virtual machines and give a screen snapshot for each step

1. FTP cracking using : Hydra, Ncrack, , Medusa, and Metasploite

https://www.hackingarticles.in/6-ways-to-hack-ftp-login-password/

2 Use Telnet to test SMTP

https://docs.microsoft.com/en-us/exchange/mail-flow/test-smtp-with-telnet?view=exchserver-2019

3. Nessus : perform the steps using your Metasploitable Machine

https://www.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus

For (4-5) follow the steps and use the given domain names

4. DNS Enumeration

https://securitytrails.com/blog/dns-enumeration

5. DNS hacking

https://resources.infosecinstitute.com/dns-hacking/#gref