SECURITY ATTACK & DEFENSE

Core Project

By

Name of the student:	Enrolment/Registration No.
Anant Kaul	1800201C202
Shreyansh Anchlia	1800185C202
Kishor Sarswat	1800228C202

Prepared in the partial fulfillment of the

Security Attack & Defense Internal Component (Core Project)

BML MUNJAL UNIVERSITY

FROM HERE TO THE WORLD

BML MUNJAL UNIVERSITY

Date of Submission: 7th May, 2021

Submitted To: Dr. Rajesh Yadav
[Asst. Prof.]
[SOET]

ASK.ME

ASK MiM Extraction System

Anant Kaul
Shreyansh Anchlia
Kishor Sarswat

(ask.me.mitm@gmail.com)
GitHub Repository Link

BACKGROUND

A man-in-the-middle attack is a type of cyber-attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM. There are various types of man-in-the-middle attacks as follows:

- Rogue Access Point
- ARP Spoofing
- mDNS Spoofing
- DNS Spoofing

So, our tool aims to protect our users from such types of attacks, which can be very harmful for any type of organisation/ company or a simple user as well (personal information is the main concern).

In the world, full of Attackers & Hackers, we here, are the Defenders.

AGENDA

The main aim for a secured environment is just a simple trick which can be performed using a windows command prompt. But the speciality of our tool is to give the users an environment that runs at the background (ghost mode) without any interrupt unless there is a serious trouble, which can in turn harm your system as well as your organisation/ company or any sort of personal information like login credentials, card details and many more.

HOW IT WORKS

This works on the principle that when a MiM attack is initiated with you, the 'Default Gateway' of the machine changes.

ASK.ME constantly detects & monitors the network traffic flow using the ARP tables (built-in) in the Microsoft Windows Operating System.

An alert is sent whenever Intrusion is detected. In addition to that, also tries to secure your environment by suggesting relevant prevention steps, giving it a title of Intrusion Prevention System (IPS).

DOCUMENTAION

How to secure you environment using ASK.ME IDS:-

- If using GUI, Run as Administrator 'ASKME.exe'.
- If using CLI, Run as Administrator 'ASK_ME_64_Win_In.exe' for 64bit Windows system & 'ASK_ME_32_Win_In.exe' for 32bit Windows system.

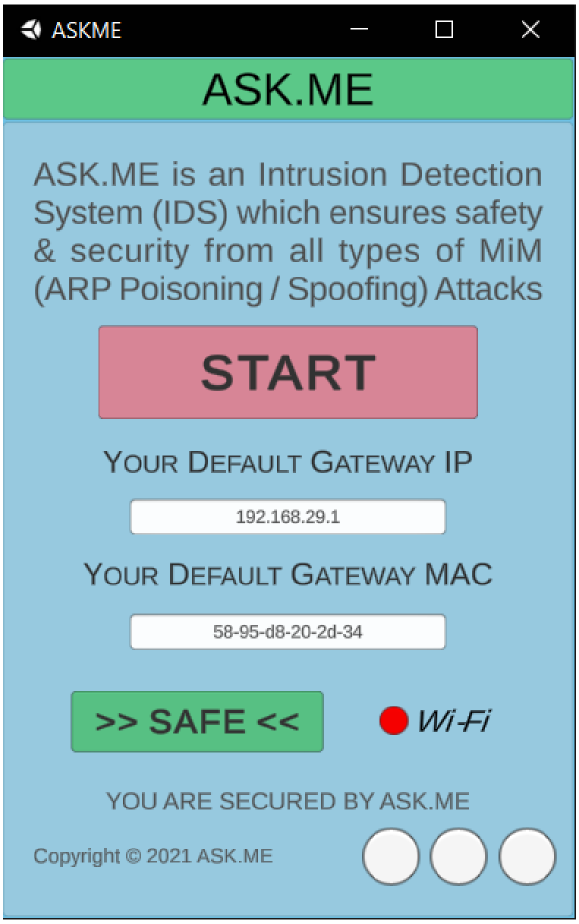
Conventional Source files (VBscript & Batch files in a sequence):-

1. run_GetIP_WiFi.vbs
   Starts the program & calls get_ip_WiFi.bat to run in the Background.
2. get_ip_WiFi.bat
   Checks the 'Default Gateway IP & MAC Address' every 3 seconds (which can be customized) & starts start_prompt_starter.vbs if the values are detected to be changed. Also, saves the output in a newly generated 'IP' directory in the 'src' directory.
3. start_prompt_starter.vbs
   Runs prompt_starter.bat.
4. prompt_starter.bat
   Runs yes_no_prompt.vbs.
5. yes_no_prompt.vbs
   Prompts a 'Yes/No prompt' and asks if the user changed the network. If the user didn't change the network, it is hence a 'MITM Attack' (ARP Poisoning Attack) & the user gets notified by calling MIMConfirmed.bat & giving it a safety tip by asking to disable Wi-Fi (WiFi_Off.bat). On the other hand, if the user selects 'Yes', then the user is stated to be safe.
6. WiFi_Off.bat
   Disables the 'Wi-Fi' as a safety tip to prevent from data leak as detected by 'ASK.ME'.
7. MIMConfirmed.bat
   Generates a 'N-Map report' in a newly generated 'NMap' directory in the 'src' directory by performing a 'Quick Scan Plus' of the network & hence, calls SendMail.vbs for the final step (generating & sending an e-mail to the user which can further be used for tracing the hacker).
8. SendMail.vbs
   Sends the generated 'N-Map report' to the specified email address (as asked by the prompt) from ask.me.mitm@gmail.com (support by ASK.ME).

ASK.ME as a Saviour in user-friendly GUI:-

1. Start Button
   After staring the application click on the 'start button' to run ASK.ME as a process. Any change in the IP/MAC address is automatically detected.

2. **Terminate Button**
   If the ASK.ME IDS system is active, it'll keep on detecting any suspicious activities. Hence, will show the terminate button to finally stop the process.
3. **Wi-Fi Toggle Button**
   This feature enhances the security of ASK.ME by providing an extra layer of security by allowing the user to enable/disable the Wi-Fi state at the administrative level.
4. **Hacker's N-Map Output Button**
   After detecting the hacker or any suspicious activity in the network, an Nmap scan is automatically performed in the background, output of which is stored in the 'nmap' directory as a text file. With the help of this button, the user can directly go to that directory and see the output as captured. The latest output is always captured in the lexicographically latest incremented text file.
5. **Default Gateway IP Info**
   Constantly scanning the arp tables, this displays the lastest (current) Default Gateway IP address of the host.
6. **Default Gateway MAC Info**
   Constantly scanning the arp tables, this displays the lastest (current) Default Gateway MAC address of the host.



ASK.ME is an Intrusion Detection System (IDS) which ensures safety & security from all types of MiM (ARP Poisoning / Spoofing) Attacks

YOUR DEFAULT GATEWAY IP: 192.168.29.1

YOUR DEFAULT GATEWAY MAC: 58-95-d8-20-2d-34

Fig. 1. ASK.ME GUI