TÉCNICAS DE SUPLANTACIÓN EN REDES AD HOC

Daniel Diaz Figueredo, Estudiante
Marcela Mejia Fajardo, PhD., Tutor.

Universidad Militar Nueva Granada
Facultad de Ingeniería
Ingeniería en Telecomunicaciones
2016

La información sumin
istrada en este documento es de carácter académico y se recomienda tener en cuenta la ley colombiana 1273 de delitos informáticos.

I. INTRODUCCIÓN

Actualmente los sistemas inalámbricos representan el soporte de transmisión más desarrollado y utilizado en el mundo de las comunicaciones, pues las ventajas que ofrece una red inalámbrica en comparación con una red cableada son realmente significativas, sin embargo no ha sido posible aprovecharlas al máximo o disponer de éstas en su totalidad, debido principalmente a que no se cuenta con la protección adecuada para dichos sistemas y por no necesitar de un medio físico son mucho más vulnerables a cualquier tipo de ataque informático.

Un claro ejemplo de lo que es una red inalámbrica es la la red ad hoc móvil (MANET, por sus siglas en inglés Mobile Ad hoc NETwork), la cual constituye una red temporal que no cuenta con administración centralizada ni con la ayuda de ninguna infraestructura preestablecida (como puntos de acceso WiFi o torres de estaciones base celulares con antenas 2G o 3G), esto permite que se pueda configurar y desplegar rápidamente cuando sea necesario. [1]

Para contribuir al desarrollo de las comunicaciones es preciso erradicar o por lo menos minimizar el efecto que tienen los nodos o estaciones de trabajo maliciosos en una red inalámbrica en particular en una red ad hoc, ya que estos nodos son usados como sustitutos para poder utilizar recursos de red que no se encuentran disponibles, afectando gravemente el funcionamiento del sistema. Lo nodos maliciosos consiguen privilegios que posee una estación de trabajo autorizada, logrando de esa manera el robo o introducción de información o enrutamiento, la suplantación de identidad, entre otras. [2]
En este tipo de redes se pueden presentar diferentes ataques de suplantación siendo estos los más comunes y representativos los que se explican a continuación.

II. ATAQUES DE SUPLANTACION

A. Man in the middle (MITM)

Este ataque fue originado en la conferencia BlackHat 2002 en las vegas por medio de un ataque llamado “Monkey-Jack”.

Para ejecutar el ataque, el intruso se ubica entre los dos host como un nodo perteneciente a la red. Una vez se establece este atacante cuenta con la facilidad de realizar ataques multicapa, por la tanto se puede considerar un ataque pasivo o activo, según la magnitud del ataque, además de tener la capacidad de leer y/o modificar información. Este ataque es comúnmente usado para la captura de claves cuando la seguridad de la red es baja y no cuenta con ninguno método de autenticación (WEP, WAP, WAP2) el cual cifre la clave.

- Detección y prevención de intrusos para el ataque MITM

Una manera de detectar los intrusos en una red ad hoc es por medio de detección de señales en los nodos de la red a nivel local. La detección de señales monitorea constantemente que equipo está ingresando a la red y que función está cumpliendo, una de las formas para determinar si hay un atacante en el miedo es haciendo test de latencia, este test no debe sobrepasar un tiempo de respuesta mayor, al que se estableció inicialmente al momento de la creación de la red. Si el tiempo de respuesta es mayor se puede deducir que un equipo está obteniendo información [2].Aunque esto aplica más para redes con infraestructura, es posible implementarlo en redes ad hoc por medio de un nodo ya establecido en la red el cual realice este test de latencia.

Otra forma para prevenir la obtención de información en este ataque es por medio de canales seguros, el cual encriptara toda información que viaje por este, a este canal solo se tiene acceso con una llave de cifrado.

B. Sybil

Sybil consiste en corromper una red por medio de la creación de múltiples usuarios falsos, este nodo malicioso intenta aislar ciertos nodos y anula la información de estos en la red, este también tiene la opción de modificar la información de los nodos por los que encamine los paquetes hasta llegar al nodo destino.

Los paquetes que se dirigen a los respectivos nodos son redirigidos al nodo sybil permitiendo la captura de información. Una vez es capturada la información, el nodo sybil realizar un ciclo de reenvió de paquetes a los nodos origen causando una saturación de paquetes en la red. Este ataque se realiza a nivel de la capa de red. [3]

- Detección de un atacante Sybil

Por medio de un agente de monitoreo, el cual es un nodo que forma parte de la red, puede ser detectado un atacante sybil al medir los saltos desde el agente hacia un nodo receptor, esto consiste en que si la distancia entre nodos es muy pequeña, se puede llegar a intuir que ambos host están en el mismo nodo, detectando cambios físicos de la señal enviada por el nodo, enviando paquete de pruebas.

La forma descrita anteriormente para identificar el atacante cuenta con una desventaja, esto se debe al momento de medir los saltos en el receptor puesto que si los nodos de la red se encuentran muy cerca podrían ser tomados como nodos atacantes.

C. Spoofing

Esta técnica de suplantación se puede clasifican según la tecnología utilizada o la capa de red afectada. A continuación se muestran los diferentes tipos de ataques spoofing. [4]

- IP/MAC Spoofing

  Al ser un medio inalámbrico se vuelve más fácil para los atacantes interceptar las comunicaciones e identificar las direcciones IP y MAC del nodo que se quiere suplantar [4].

  El ataque IP Spoofing se encarga de falsificar la dirección IP/MAC obtenida anteriormente por un escaneo a la red o realizando un ataque MITM. Esta dirección IP y MAC son establecidas en un nuevo nodo fuera de la red el cual se encargara de suplantar al nodo autenticado.

- ARP Spoofing

  Esta es un técnica hacking que se usa para infiltrarse en la red. Esta técnica se realiza con el fin de obtener información de los clientes de la red tales como lo son: nombre de usuario, cookies, captura de mensajes entre otros. [5]

  Para realizar esto se generan mensajes ARP sobre la red, indicando que la MAC del atacante está asociada a la IP de la víctima, y a la del nodo inalámbrico solicitante que requiera el uso ARP de la red. Este mensaje causara que las máquinas de la red actualicen su información en las tablas. Esto comprenderá que al enviar un paquete hacia el router este paquete será enviado al host malicioso. [5]

- DNS Spoofing

  El ataque DNS spoofing hace referencia a una falsificación de IP, al realizar una consulta de resolución de nombre, esto quiere decir que se resuelve por medio de una dirección IP falsa un nombre DNS, Esta dirección IP falsa está conectada a un servidor que está siendo controlado por los atacantes [6].

  Como método de protección para este ataque se requiere modificar las entradas al servidor de manera segura, esto se realiza por medio de cookies a los host solicitantes que requieren acceder al DNS. El servidor tendrá que validar la dirección de origen identificando el paquete a través de la cookie asignada.

D. Sinkhole

Sinkhole es un ataque dedicado a cambiar las rutas de origen/destino, este ataque se basa en falsificar las rutas de los paquetes, atrayéndolas a un nodo malicioso comenzando un bajo funcionamiento en la red puesto que todos los paquetes comenzaran a tomar la misma ruta.[7]

Un esquema para la protección de la red es la implementación de agentes móviles, este es un programa el cual se instala en los nodos antes de ingresar a la red. En esta instalación se establece un tipo de cifrado. Permitiendo realizar un control nodo a nodo de la transmisión de datos de tal modo que si un nodo no autorizado captura la información esta no podrá ser legible. Estos agentes también realizan cálculos constantes de los saltos a realizar en la red y la verificación del cifrado de tal forma que si un nodo no cuenta con el cifrado este puede ser considerado como un nodo sinkhole.

E. Hijacking

En este tipo de ataque se asalta una conexión o una sesión de un usuario con el fin de generar una autenticación. Es en este momento donde se realiza la suplantación y se procede a la configuración de la dirección IP esto genera una respuesta por parte del nodo atacado la cual genera una conexión TCP entregándole un número de secuencia[8].

Al tener esta información el nodo atacante ejerce el control de la sesión y tiene liberta para ejercer cualquier tipo de daño en la red, tanto él envió de tramas para saturar la red, obtención de información hasta la negación del servicio.

Con el fin de generar una mitigación en este tipo de ataques, se ha establecidos protocolos de autenticación, estos protocolos manejan encriptación en la conexiones con el fin de dificultar la suplantación en las sesiones establecidas. [8]

III. ESCENARIO

Se implementó un escenario de prueba de una red ad hoc conformada por 3 usuarios. Adicionalmente se utilizaron 2 equipos externos a la red con los cuales se realiza el ataque, y la recolección de información.

Ya con la red funcionando se procede a realizar una captura de información del objetivo a atacar, por medio del software kali Linux el cual se explicara detalladamente más adelante.

Para este caso eran necesarias: MAC, IP y credenciales de uno de los host de la red. Cuando se obtenga esta información se procede a realizar el ataque de suplantación.

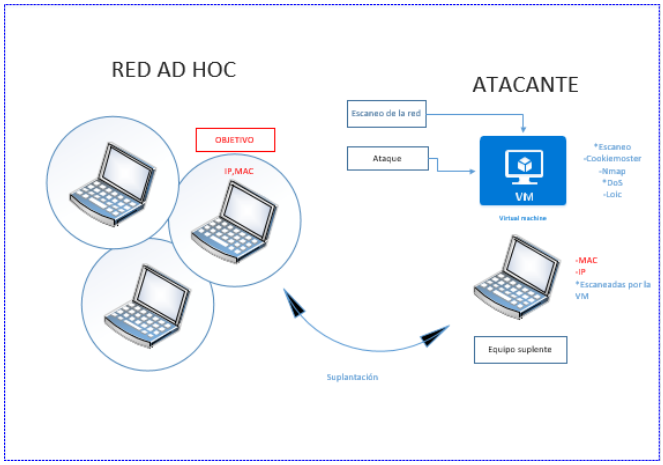

Figura 1. Escenario propuesto

A. PROCEDIMIENTO

Primero se creó la red ad Hoc la cual se estableció con 3 host Windows, para la creación de esta red fue necesario el uso de las tarjetas inalámbricas de los equipos y se estableció la red por medio de comandos de consola (cmd) como lo indican los siguientes pasos:

1) Para establecer la red se ingresara a la consola de Windows y se escribirá el siguiente comando

- netsh wlan set hostednetwork mode=allow ssid=”Nombre de la Red” key=”clave”

En este comando se establece el SSID el cual corresponde al nombre de la red que para este caso se llamara “Ad_hoc”. Key corresponde a la clave la cual contara con seguridad WPA2/PSK y para este caso se le asignara una contraseña cuenta con especificaciones seguras debido que contiene: números, letras en mayúsculas, caracteres especiales, y minúsculas.[9]

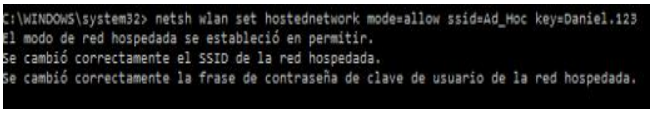

Figura 2. Creación de la red ad hoc

Una vez se cree la red, Se generara un mensaje notificando que la red se ha creado correctamente en el equipo. Ahora se inicia la red que se acaba de crear para que los demás host puedan conectarse y compartir datos.

2) Iniciación de la red creada por medio de comandos en CMD

- *netsh wlan start hostednetwork*

Por medio de este comando se inicia la red la cual se creó previamente y este notificara que la red se inició con éxito.

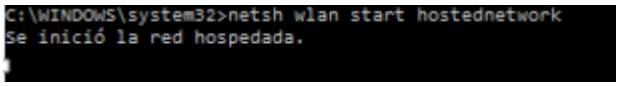

Figura 3. Inicio de la red

Una vez se tiene la red creada e iniciada se puede establecer una direccion IP y mascara para esta, aunque al ser creada en windows este crea una direccion IP automatica y crea un servidor de direcciones por DHCP. Para este caso se usara la direccion IP 192.168.137.1 que funcionara como puerta de enlace con una mascara 255.255.255.0

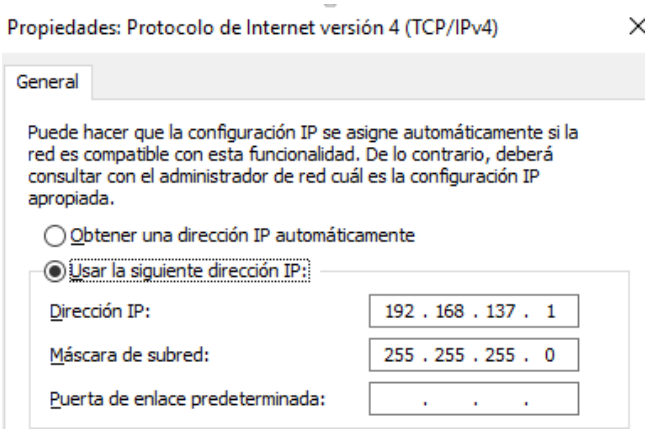

Figura 5. Dirección IP

3) Recolección de información de la red a atacar por medio de un host con sistema operático kali linux

Este ataque se realiza a través de la herramienta aircrack, lo primero a realizar es activar la tarjeta de red en modo monitor, esto se realiza por medio del comando “airmon-ng start wlan0”.

Una ves se tiene la tarjeta en modo monitor se procede a escuchar las diferentes redes inalambricas que se encuntran en el aerea de cobertura de la tarjeta, para eso se usara el comando “airodump-ng wlan0mon”. Como se puede ver en la Figura 7 se indentificara la red a la cual se le quiere realizar el ataque que para este caso es la red que se creo con el nombre “Ad_Hoc”.

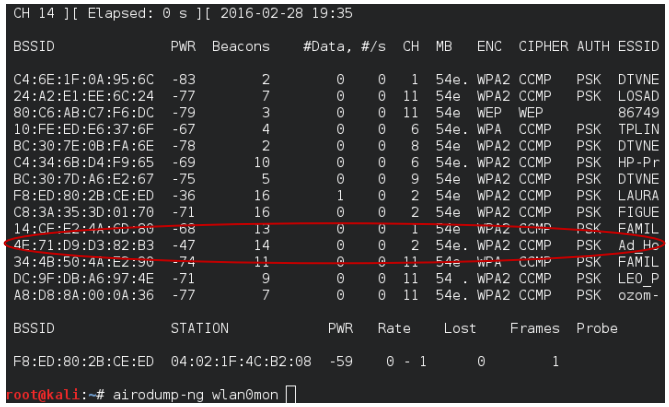

Figura 7. Escaneo de las redes

Una vez realizado este escaneo se comenzara a obtener la informacion necesaria para realizar el ataque, es bien importante identificar los siguientes aspectos: BSSID, CH,ENC,AUTH.

BSSID: Indica la MAC del punto de acceso a la red

CH: Canal de la red

ENC: Tipo de seguridad de la red

AUTH: Tipo de autenticación de la red

Cuando ya se tiene esta informacion se realiza una busqueda mas especifica de la red a atacar, para eso se vuelve a usar el comando airodump especificando la informacion obtenia. Para este caso se escribira “airodump-ng –c 2 –bssid 4E:71:D9:D3:82:B3 wlan0mon”.

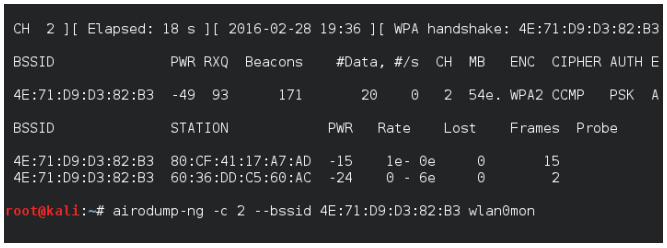

Figura 8.Escaneo de la red específica a atacar.

Una vez se esté escaneando la red este mostrara los dispositivos que estén conectados por medio de este BSSID. Esto se realiza con el fin de enviar un mensaje desautenticando los equipos conectados por un instante de tiempo.

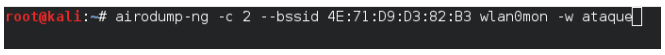

Figura 9. Crear archivo de datos recolectados

Esta información será guardada en un archivo .cap por medio del comando –w al cual se le asignara un nombre como se muestra en la figura 9.

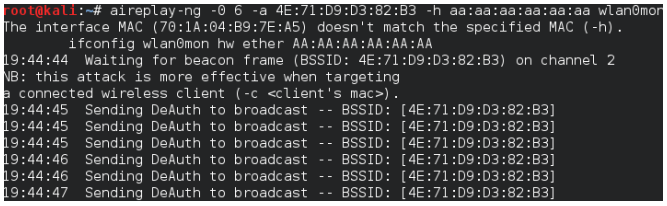

Figura 10. Mensaje de desautenticacion

Haciendo uso de la herramienta aireplay-ng se enviara el mensaje de desautenticacion de la siguiente manera “aireplay-ng -0 6 –a 4E:71:D9:D3:82:B3 –h aa:aa:aa:aa:aa:aa wlan0mon” , el numero 6 sera la cantidad de mensajes que se enviaran para desautenticar los dispositivos conectados, la opción –a indica la MAC del punto de conexión y –h será una MAC cualquiera con la cual se esconderá el mensaje de desautenticacion.

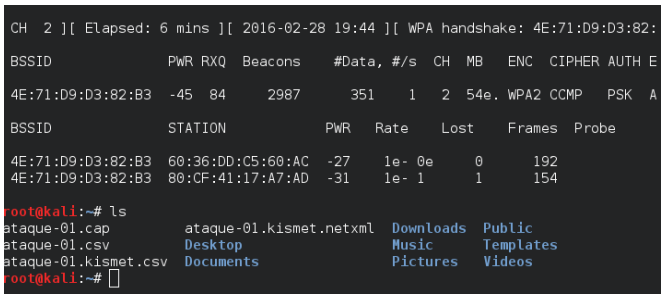

Figura 11. Mensajae WPA Handshake

Este mensaje es enviado con el fin de generar un handshake este mensaje es el encargado de generar un saludo de autenticación cuando se conecta un equipo a la red.

La desautenticacion y la autenticación se realizan para obtener la captura de la clave en el archivo creado que para este caso fue llamado con el nombre “ataque”,

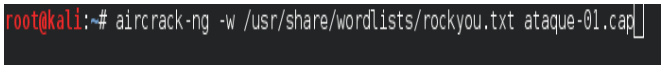

Figura 12. Búsqueda de clave

Para encontrar la clave se hace uso de la herramienta aircrack-ng por medio de un diccionario de claves WPA2. El cual cuenta con 73 millones de claves,

Para realizar la suplantación del equipo se suplanto el equipo con dirección MAC 60:36:DD:C5:60:AC, para eso se cambio la dirección MAC en el equipo suplente.

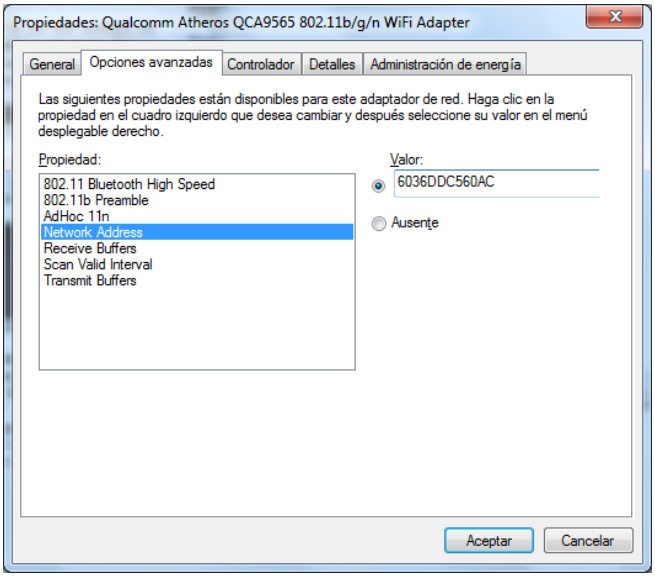

Figura 14.Cambio dirección MAC

También es necesario establecer la dirección IP que tiene el equipo a suplantar, la cual se obtuvo anteriormente por la herramienta netdiscover la cual permitió capturar la dirección IP del equipo

IV. ANALISIS DE RESULTADOS

Por medio de este trabajo se demuestra que al realizar el ataque en una arquitectura descentralizada, y establecer las tarjetas de red en modo promiscuo, permiten realizar una captura de información como lo son: MAC, IP y BSSID.

Se comprobó que al realizar un ataque con una contraseña poco segura, se evidencio que el tiempo para encontrar la clave fue de tan solo unos minuto mientas que al realizar el mismo ataque con una clave más robusta este tiempo se extendió durante varias horas.

Este tiempo de respuesta se debe a que en la primera contraseña se maneja una palabra predecible y alfanumérica. En la segunda contraseña se manejan caracteres en mayúsculas y números sin ninguna coherencia alfabética ni secuencial, generando una contraseña más segura si se realiza un ataque de diccionario como en este caso.

Otra de las cosas a analizar es que al tener una red inalámbrica creada desde un host esta cuenta con un déficit de infraestructura de seguridad, permitiendo tener la capacidad de enviar paquetes de desautenticacion, como se realizó en el procedimiento por medio de la herramienta aireplay-ng.

Al momento de realizar el ataque por diccionario este dependerá de la cantidad de claves en el archivo e idioma en el que se descargue, con esto se quiere decir que si se está realizando un ataque en España y el diccionario esta en inglés es muy poco probable que el ataque tenga éxito.

V. CONCLUSIONES

Por medio de la creación de las redes ad hoc se permite desplegar y adaptar, un entorno de trabajo inalámbrico en cualquier espacio. Sin tener la complejidad de una infraestructura definida.

La realización del escenario permitió concluir que el manejo de contraseñas es de vital importancia a la hora de querer brindar una seguridad más robusta a la red. Para esto es posible apoyarse en la creación de contraseñas seguras las cuales deben tener como mínimo 8 caracteres entre esos tiene que contar con mayúsculas minúsculas y caracteres especiales.

Para esto también es necesario tener una configuración avanzada, lo cual indica que se tendrá que manejar una contraseña WPA2 el cual maneja los últimos estándares de seguridad con los tipos de encriptación. Esto puede ser una ayuda para proteger las redes ad hoc ya que estas son redes temporales que se establecen cuando no existe una infraestructura definida.

Por último se logra concluir que al realizar un ataque no siempre se tiene el 100 % de efectividad, puesto que es necesario cumplir con los lo son compatibilidad de la tarjeta de red en modo monitor, soporte del sistema operativo para este caso fue kali linux. También es fundamental entender el funcionamiento de la red, Tipo de seguridad (WEP, WPA2), cobertura, Tipo de red ya sea ad hoc o de infraestructura. Esto con el fin de entender la red que se está atacando para determinar las vulnerabilidades que tiene y poder explotarla al máximo

VI. REFERENCIAS

[1]S. H. r. Moreo, *CASO DE ESTUDIO DE COMUNICACIONES SEGURAS SOBRE REDES MOVILES AD HOC,* La Plata, 2013.

[2] Peral, B. (2008), 'CONTROL DE TOPOLOGÍA SOPORTADO POR TÉCNICAS DE CLUSTERING APLICADO A REDES AD HOC', PhD thesis, Universidad Complutense.

[3]Hazra, S. & Setua, S. (2012), Sybil attack defending trusted AODV in ad-hoc netwok, *in* 'Computer Science and Network Technology (ICCSNT), 2012 2nd International Conference on', pp. 643-647.

[4]Chen, Y.; Trappe, W. & Martin, R. (2007), Detecting and Localizing Wireless Spoofing Attacks, *in* 'Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on', pp. 193-202.

[5]Sharma, D.; Khan, O. & Manchanda, N. (2014), Detection of ARP Spoofing: A command line execution method, *in* 'Computing for Sustainable Global Development (INDIACom), 2014 International Conference on', pp. 861-864.

[6]Guo, F.; Chen, J. & cker Chiueh, T. (2006), Spoof Detection for Preventing DoS Attacks against DNS Servers, *in* 'Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on', pp. 37-37.

[7]Gandhewar, N. & Patel, R. (2012), Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network, *in* 'Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on', pp. 714-718.

[8]PRADIP M. JAWANDHIYA, MANGESH M. GHONGE, D. M. P. J. D. (2010), 'A Survey of Mobile Ad Hoc Network Attacks.', *International Journal of Engineering Science and Technology*

[9] C. M. Chen and T. H. Chang, "The Cryptanalysis of WPA & WPA2 in the Rule-Based Brute Force Attack, an Advanced and Efficient Method," *Information Security (AsiaJCIS), 2015 10th Asia Joint Conference on*, Kaohsiung, 2015, pp. 37-41.
doi: 10.1109/AsiaJCIS.2015.14

[10] M. M. Hafiz and F. H. Mohd Ali, "Profiling and mitigating brute force attack in home wireless LAN," *Computational Science and Technology (ICCST), 2014 International Conference on*, Kota Kinabalu, 2014, pp. 1-6.
doi: 10.1109/ICCST.2014.7045190