Inside this Issue Vol 3: issue 2/19

Cyber Tips

How to stay safe on line.

Cybercriminals have become quite savvy in their attempts to lure people in and get you to click on a link or open an attachment.Read more >>

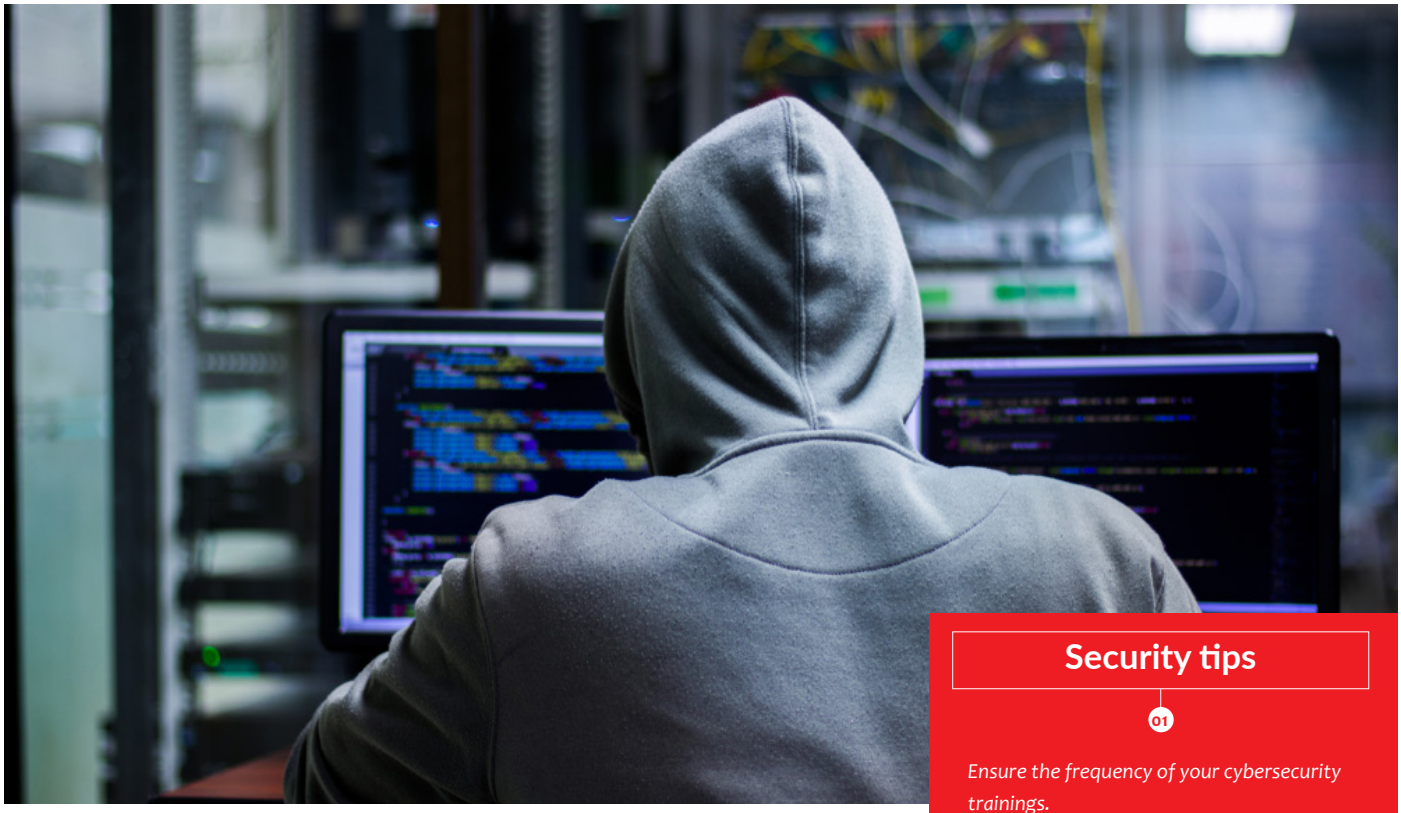
BCP/DR for cybersecurity

Make a Cybersecurity BCP/ DR policy as part of the organization's overall BCP/DR plan. A formal policy signed and approved by the board and guidance necessary to develop an effective plan is the first step is making contingency planning part and parcel of the organization.>>

Institute Of Forensics & ICT Security www.forensicsinstitute.org

Forensics & **Cyber Security** Newsletter

Your source of forensics, security and fraud insights



The Unexpected cyber threats: Man-in-the-Middle Attacks

Online communication involves two people or organizations doing business through messages sent over an internet connection. The expectation is that nobody is listening to the traffic on that connection. And messages are encrypted so that interceptors don't understand, but this is not usually the case.

A man in the middle attack (MITM), is a form of cyber-attack in which the attacker inserts himself or herself into the connection, routing traffic from each of the participants to the other and reading it as it passes through.

This is one of the most dangerous and effective attacks that can be used, it is used to redirect packets to and from any client to the attacker's device, and if the attacker is in the same network, they can read/modify/drop these packets. allows them to launch very powerful attacks. MITM attacks are very effective

Security tips

01

Ensure the frequency of your cybersecurity trainings.

"Cybersecurity training has to be provided to every employee (including C-Suite) at least twice a year. This frequency will increase awareness and allow the company a chance to update employees on how to identify the latest threats."

02

Always perform financial transactions on a secure computer, use dual authentication, and never perform banking from an open source such as an Android phone.

and dangerous as they exploit the insecure way that Address Resolution Protocol (ARP) works.

ARP has two main issues,

a. Each ARP request/response is trusted. This means that whatever the attackers device says to other devices in the same network will be trusted without further authentication.

b. Clients can accept responses even if they didn't send the request. When a device connects to the internet, the first question it will ask is "who is the router". If a MITM attack is in progress the attacker will then respond "I am the router" and the device will thus start sending data packets.

c. MITM attacks work by using a technique called ARP poisoning/ ARP spoofing which is done by exploiting the two issues above.

One of the main tools used for MITM attacks is called Man in the Middle Framework (MITMf). It makes ARP spoofing while providing a catalog of very many other useful tools.

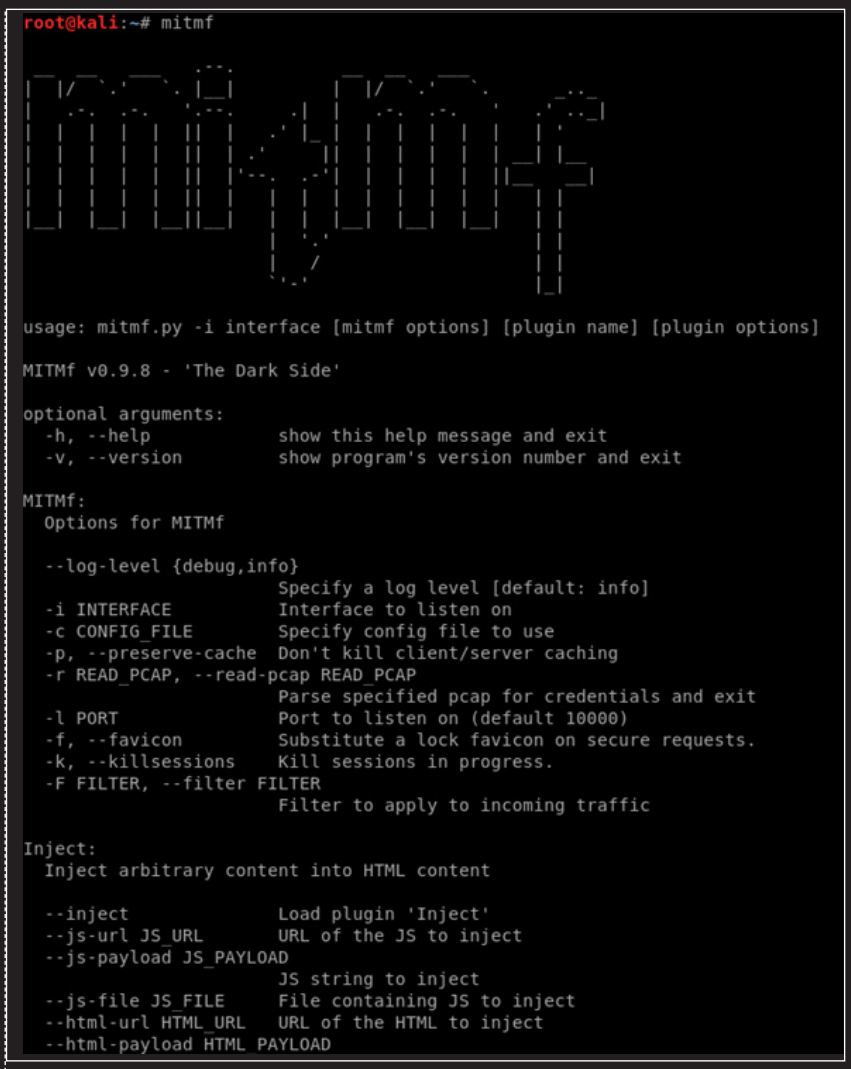


Figure 2: Man in the Middle framework (MITMf)

Figure 2: Man in the Middle framework (MITMf)

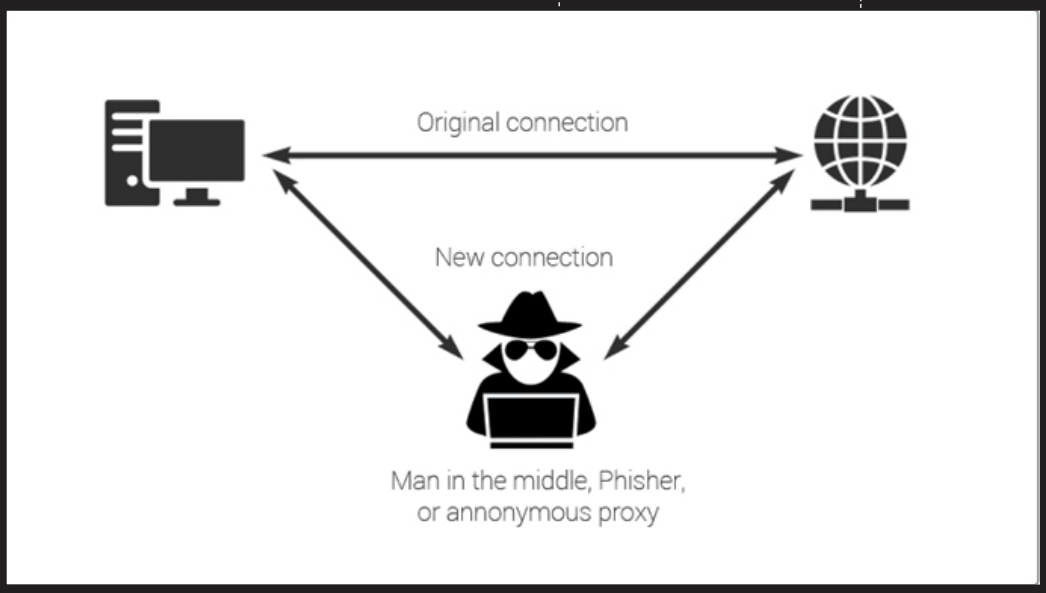
What next in the midst of MITM Attacks

To combat these attacks, many organizations have implemented end-to-end connection security on their internet communications using Secure Hypertext Transport Protocol (HTTPS). In addition,
some organizations use "HTTPS interception products" to detect malware over an HTTPS connection. These products work by intercepting the HTTPS network traffic and decrypting it, reviewing it, then re-encrypting it. To do so, HTTPS interception products must install trusted certificates on client devices to achieve the HTTPS inspection without presenting warnings.

some organizations use "HTTPS interception products" to detect malware over an HTTPS connection.

However, this process may leave organizations using HTTPS interception products vulnerable, because the organizations can no longer verify web servers' certificates, view the protocols and ciphers that an HTTPS interception product negotiates with web servers, and, most importantly, independently validate the security

Figure 1: MITM attack layout



All in all, the organizations that use these interception products are able to validate only the connection between themselves and the interception product, not between themselves and the server. This is problematic, because many HTTPS interception products do not properly verify the certificate chain before re-encrypting and forwarding information to the organizations, which leaves the connection vulnerable to a malicious MITM attack.

Man In The Middle Attack Prevention

a) For Individuals

i. Do not use open wi-fi networks

ii. Pay close attention to browser notifications that say the site is insecure

iii. Log out of applications when not in use

iv. When connected to a public network, refrain from financial transactions online.

b) For Website Operators

i. Use of TLS and HTTPS in addition to SSL to protect each and every page.

c) For Organizations

i. Use an email security solution

ii. Use web security solutions

iii. Employee education and trainings

iv. Review user credentials often.

v. Detect ARP poisoning attacks by using applications like XArp.

vi. Have network administrators who are well versed with Wireshark as it has very many options for packet analysis including detecting suspicious network activities.

Security tips

03

Make certain your home Wi-Fi and IoT [Internet of Things] devices are secure. Adopt the WPA security and have a complex password (no home address or name) for your home Wi-Fi, and make certain all your IoT (thermostats, cameras, security systems) have new passwords you provided them—not the default passwords.

04

Keep your antivirus and firewalls up to date on ALL your devices—regardless of internet connectivity. Malware is everywhere today—phones are the latest target!

Cybersecurity BCP/DR Planning

The Institute of Forensics and ICT Security (IFIS) has been providing training to organizations in setting up an effective Business Continuity and Disaster Recovery plan (BCP/DR) as an overall coverage for contingency planning. Experience has shown that organizations do not include procedures for handling a BCP/DR training and those organizations that had these plans, they didn't include procedures for a cyberattack indicating a gap in the knowledge and importance of contingency planning.

The purpose of any contingency plan is to let an organization recover and maintain daily operations as quickly as possible after an unpredicted event. The plan protects resources, minimizes customer inconvenience and identifies key staff, assigning specific responsibilities in the context of the recovery. BCP/DR Plans should consider not only how to respond to disasters such as fires and floods, but also how to respond to cyberattacks.

BCP/DR for cybersecurity

BCP/DR plans are critical to protecting the availability, integrity, and security of data during unexpected antagonistic events.

Cyberattacks using malicious software such as ransomware may render an organization's data unreadable or unusable. In the event data is compromised due to a cyberattack, restoring the data from backups may be the only option to recover the data and restore normal business operations.

What Does a cybersecurity BCP/DR do?

A BCP/DR plan is focused on the steps to respond and recover operations in the event of an emergency or other disruption to normal operations. Its major aims are to guarantee:

- the containment of damage or injury to, or loss of, property, personnel, and data; and
- the continuity of the key operations of the organization.

What does a good Cybersecurity BCP/DR plan entail?

1. Disaster Recovery Plan (DRP): This is focused on restoring an organization's protected confidential data.
2. Business Continuity Plan (BCP): This plan is focused on maintaining and protecting critical functions that protect the security of protected confidential data.
3. Data Backup Plan (DBP): As part of the BCP, this plan is fixated on regularly copying protected data to ensure it can be restored in the event of a loss or disruption.

To read more visit: https://www.forensicsinstitute.org/cybersecurity-bcp-dr-planning/

IFIS
Institute of Forensics & ICT Security
Forensics. Security. Training

Transform Your Career with a

DIPLOMA in INFORMATION SECURITY & COMPUTER FORENSICS

Attain the skills in high demand by every employer

contact us on 4th Foor, Block B, Ntinda Complex
Plot 33, Ntinda Road Opp St Luke Church,
P.O. Box 40292, Kampala, Uganda
M: 256(414) 231136
E:admissions@forensicsinstitute.org

Visit >> www.forensics**institute**.org to enroll

This **Diploma in Information Security & Computer Forensics (DISCoF)** will give you the requisite skillsets to design, deploy and manage security architecture for your organization.

Get the skills in demand today. Become a DISCoF today

DIPLOMA in INFORMATION SECURITY & COMPUTER FORENSICS

With Practical Skills, You Succeed