

Forum:[Hack Forums](#)

Thread: [A question about MitM attacks](#)

jasonnix - February 27, 2025, 12:23 pm

Hello,

I have a question about MitM attacks. As the name suggests, the hacker is placed between the user and the destination. Suppose a web application like GitLab uses the HTTP protocol. When the hacker places himself between the user and the GitLab server to perform a MitM attack, where is this middleman? Is it the router that the user uses to reach the destination via the Internet?

Please explain simply and briefly.

Thank you.

vetbesim - February 27, 2025, 12:49 pm

No mitm: User -> router -> gitlab

Mitm: User -> hacker -> router -> gitlab

<https://www.imperva.com/learn/application-security/arp-spoofing/>

explains that the hacker lies to the user and the router, he tells the router that he is the user and he tells the user that he is the router

grady - February 27, 2025, 1:05 pm

Depends on the method of MitM.

For DNS cache poisoning/ARP cache poisoning, the traffic is redirected to the attacker and, optionally, can be proxied to the legitimate destination.

For network sniffing, you're eavesdropping on traffic in the same broadcast domain.

OtterBot - February 27, 2025, 1:27 pm

It also could be something like a pineapple, where the user connects to the hackers network. This then allows the hacker to access all traffic while the victim thinks they're on says Starbucks's network.

DramaKing - February 27, 2025, 2:14 pm

(Feb 27, 2025 01:23 PM)jasonnix Wrote: [\[CITE\]](#) Hello,

I have a question about MitM attacks. As the name suggests, the hacker is placed between the user and the destination. Suppose a web application like GitLab uses the HTTP protocol. When the hacker places himself between the user and the GitLab server to perform a MitM attack, where is this middleman? Is it the router that the user uses to reach the destination via the Internet?

Please explain simply and briefly.

Thank you.

First of all, GitLab uses HTTPS like virtually every other website. And realistically you're not doing MitM on the WAN. Datacenters have seriously high security. ARP spoofing Internet routers hasn't successfully been done in a long time. A VPN or proxy service could do it but little else.

jasonnix - April 19, 2025, 5:39 am

(Feb 27, 2025 01:49 PM)vetbesim Wrote: [\[CITE\]](#) No mitm: User -> router -> gitlab

Mitm: User -> hacker -> router -> gitlab

<https://www.imperva.com/learn/application-security/arp-spoofing/>

explains that the hacker lies to the user and the router, he tells the router that he is the user and he tells the user that he is the router

Hello,

Thank you so much for your reply.

You said:

Code User -> hacker -> router -> gitlab

What is the hacker here that the user can connect to?

(Feb 27, 2025 02:05 PM)grady Wrote: [\[CITE\]](#) Depends on the method of MitM.

For DNS cache poisoning/ARP cache poisoning, the traffic is redirected to the attacker and, optionally, can be proxied to the legitimate destination.

For network sniffing, you're eavesdropping on traffic in the same broadcast domain.

Hello,

Quote:For DNS cache poisoning/ARP cache poisoning, the traffic is redirected to the attacker and, optionally, can be proxied to the legitimate destination.

How does the hacker redirect traffic to himself? Did he hack a router?

Quote:For network sniffing, you're eavesdropping on traffic in the same broadcast domain.

The same broadcast domain? Does that mean the hacker is on the same network as the users?

vetbesim - May 2, 2025, 2:39 pm

(Apr 19, 2025 05:39 AM)jasonnix Wrote: [\[CITE\]](#) Hello,

Thank you so much for your reply.

You said:

Code User -> hacker -> router -> gitlab

What is the hacker here that the user can connect to?

Hello,

How does the hacker redirect traffic to himself? Did he hack a router?

The same broadcast domain? Does that mean the hacker is on the same network as the users?

The hacker is going to be in the same network as the victim

the hacker tells the victim that he is the router, and tells the router that he is the victim via arp spoofing, and the user sends data to the hacker, believing that he is the router. But the hacker can only view the data in insecure protocols like http, he cannot view data send to or received to/by a website using https. If I were you I'd look up what arp spoofing is so you can understand it better, and ask chatgpt if you still dont get it

DramaKing - May 2, 2025, 6:07 pm

(Apr 19, 2025 05:39 AM)jasonnix Wrote: [\[CITE\]](#) Hello,

Thank you so much for your reply.

You said:

Code User -> hacker -> router -> gitlab

What is the hacker here that the user can connect to?

Hello,

How does the hacker redirect traffic to himself? Did he hack a router?

The same broadcast domain? Does that mean the hacker is on the same network as the users? Are you really asking for someone to explain ARP poisoning to you? DNS cache poisoning is also easy to learn if you take five minutes. It's been discussed in depth here.

A broadcast domain is the same as a subnetwork, i.e. all the hosts that can send and receive broadcasts to each other. That should be obvious if you're doing MitM. All the answers are here.

jasonnix - May 4, 2025, 3:34 am

(May 2, 2025 06:07 PM)DramaKing Wrote: [\[CITE\]](#) Are you really asking for someone to explain ARP poisoning to you? DNS cache poisoning is also easy to learn if you take five minutes. It's been discussed in depth here.

A broadcast domain is the same as a subnetwork, i.e. all the hosts that can send and receive broadcasts to each other. That should be obvious if you're doing MitM. All the answers are here.

Hello,

One thing is unclear to me. If a hacker wants to do this for a home user, how should he\she impersonate the router? Would he\she have to hack the ISP?

DramaKing - May 4, 2025, 3:54 am

(May 4, 2025 03:34 AM)jasonnix Wrote: [\[CITE\]](#) Hello,

One thing is unclear to me. If a hacker wants to do this for a home user, how should he\she impersonate the router? Would he\she have to hack the ISP?

In 2025? You would need to control the ISP, although there was an in-depth thread not long ago on DNS poisoning.

You'll find that SSL/TLS remediates a lot of the classic MitM attacks.