deadlysnowman3308 / **upgraded-ARP-Poisoning** Public

An upgraded-ARP-Poisoning attack can be directed at “cheating” a host computer or a network router. If a router has the wrong MAC address for a given IP address, then all communications are routed to the wrong host.

MIT license

4 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

Hackingvila Go to file

deadlysnowman3308 Update README.md ... on Aug 14, 2021 19

View code

README.md

upgraded-ARP-Poisoning

CVE-2021-29280

After running this tool, wait for 1-2 minutes then automatically your Internet will be disconnected !!

All connected devices also can't connect to the internet.

What is ARP-Poisoning?

- ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.
- The attack itself consists of an attacker sending a false ARP reply message to the default network gateway, informing it that his or her MAC address should be associated with his or her target's IP address (and vice-versa, so his or her target's MAC is now associated with the attacker's IP address). Once the default gateway has received this message and broadcasts its changes to all other devices on the network, all of the target's traffic to any other device on the network travels through the attacker's computer, allowing the attacker to inspect or modify it before forwarding it to its real destination. Because ARP Poisoning attacks occur on such a low level, users targeted by ARP Poisoning rarely realize that their traffic is being inspected or modified. Besides Man-in-the-Middle Attacks, ARP Poisoning can be used to cause a denial-of-service condition over a LAN by simply intercepting or dropping and not forwarding the target's packets.

:: Installation ::

```
$ git clone https://github.com/deadlysnowman3308/upgraded-ARP-Poisoning

$ cd upgraded-ARP-Poisoning

$ sudo chmod +x *

$ sudo pip3 install requirements.txt
```

:: Usage ::

```
$ sudo python3 upgraded-ARP-Poisoning.py
```

- Note: After turn off this tool, your internet should be online. If not then restart your router !!

CVE-2021-29280

Created by:> Aniket Dinda

Releases

No releases published

Packages

No packages published

Languages

- **Python** 100.0%