

Forum: [Hack Forums](#)

Thread: [DHC Pain: Lease Exhaustion Utility](#)

Goodies - June 16, 2020, 1:05 pm

DHC Pain is a simple lease exhaustion utility that I developed for an independent book that I am authoring. I wanted to demonstrate some network attacks, but some tools for DHCP exhaustion are either non-functional with current software versions (DHC Pig) or do not properly exhaust leases by responding to DHCP Offer messages. For this reason, DHC Pain was created as a very simple tool to exhaust DHCP scopes of a target network. One benefit of this tool is that the source MAC address is not changed per frame, so it will not be mitigated by port security alone. Networks must be secured with DHCP snooping and MAC verification in order to properly avoid this attack.

Code pip install dhcpain

Github Link: <https://github.com/GoodiesHQ/DHCPain>

Code git clone <https://github.com/GoodiesHQ/DHCPain>

cd DHC Pain

pip install -r requirements.txt

python dhcpain.py -l

Runs on Linux and Windows:

Eats up DHCP leases on Windows Server, home routers, dhcpd, etc...

Does not modify source MAC address of the ethernet frames, so it cannot be prevented by port security alone. DHCP snooping must be enabled for protection.

Goodies - June 19, 2020, 10:27 am

No? Nobody interested in MITM via DHCP?

int13h - June 20, 2020, 3:10 pm

thank you so much! much appreciated amazing tool

ETH - June 21, 2020, 1:30 am

(Jun 19, 2020 10:27 AM)Goodies Wrote: [\[CITE\]](#) No? Nobody interested in MITM via DHCP?

Really many are interested buddy

I hope i could do some MITM on my network with this tool

Goodies - March 15, 2021, 4:04 pm

Wow what a neat tool, must have taken you a little while to code.

Hey, thanks, how kind of you!

tux1 - *March 17, 2021, 11:15 am*

Interesting tool and thanks for sharing, hope the book is coming along well!