

Forum:[Hack Forums](#)

Thread: [Infecting Computer on LAN](#)

Furz - April 7, 2023, 8:43 am

I have access to my network and want to infect other PC's on the LAN

Could someone give me an easy guide for something like this? Maybe ARP poisoning or such?

iCasher - April 7, 2023, 8:48 am

(Apr 7, 2023 08:43 AM)Furz Wrote: [\[CITE\]](#) I have access to my network and want to infect other PC's on the LAN

Could someone give me an easy guide for something like this? Maybe ARP poisoning or such?

- build your payload , encrypt it from AV's
- build fake page to SE your victims
- edit your dns to redirect all the network users to your fake download page before they go to anywebsite
- wait your victims

this is very basic and most effective way to infect other PC's on the same lan , ofc there are vulnerability's you can use and long way for checking open ports on each machine or running services etc but i suggest you the first option

National Crime Agency UK - April 18, 2023, 3:17 am

(Apr 7, 2023 08:43 AM)Furz Wrote: [\[CITE\]](#) I have access to my network and want to infect other PC's on the LAN

Could someone give me an easy guide for something like this? Maybe ARP poisoning or such?

@Furz - In your signature it mentions "In every affair consider what precedes and follows, and then undertake it." In this affair what precedes is a prison sentence.

(Apr 7, 2023 08:48 AM)iCasher Wrote: [\[CITE\]](#) - build your payload , encrypt it from AV's

- build fake page to SE your victims
- edit your dns to redirect all the network users to your fake download page before they go to anywebsite
- wait your victims

this is very basic and most effective way to infect other PC's on the same lan , ofc there are vulnerability's you can use and long way for checking open ports on each machine or running services etc but i suggest you the first option

Our advice don't do what @iCasher has described it is illegal.

Learn about UK Cyber legislation and find resources to utilise your skills legally by visiting [cyberchoices.uk](#)

Please note: This is not a crime reporting channel, to report a crime contact your local police force. If you are in the UK you can report fraud and cyber crime at Action Fraud UK.

Sand Ferret - April 18, 2023, 3:50 am

(Apr 18, 2023 03:17 AM)National Crime Agency UK Wrote: [\[CITE\]](#) @Furz - In your signature it

mentions "In every affair consider what precedes and follows, and then undertake it." In this affair what precedes is a prison sentence.

Our advice don't do what @iCasher has described it is illegal.

Learn about UK Cyber legislation and find resources to utilise your skills legally by visiting cyberchoices.uk

Please note: This is not a crime reporting channel, to report a crime contact your local police force. If you are in the UK you can report fraud and cyber crime at Action Fraud UK.
Jesus Christ reading your replies is painful.

Dread.Reaper - April 18, 2023, 4:17 am

(Apr 18, 2023 03:50 AM)Sand Ferret Wrote: [\[CITE\]](#) Jesus Christ reading your replies is painful.

?

Yea but you gotta give them some credit for their scare tactics. On. Every. Single. Fucking. Aspect.

(Apr 18, 2023 03:17 AM)National Crime Agency UK Wrote: [\[CITE\]](#) @Furz - In your signature it mentions "In every affair consider what precedes and follows, and then undertake it." In this affair what precedes is a prison sentence.

Like holy shit bruh... Someone give them a Dilaudid. ???

DramaKing - April 18, 2023, 8:25 am

(Apr 7, 2023 08:43 AM)Furz Wrote: [\[CITE\]](#) I have access to my network and want to infect other PC's on the LAN

Could someone give me an easy guide for something like this? Maybe ARP poisoning or such?

There's no easy way to infect PC's with ARP poisoning. A tool like Backdoor Factory can be made to inject malware into PE's. I think I have a GitHub repo saved with a fork of BdF designed to integrate with bettercap, not that I've ever figured it out. If you want to make the exercise realistic, any detectable signatures in the payload will still be detected by AV. This will also only work on unsigned Windows executables or unsigned Linux packages.

I prefer password attacks and RCE to infect PC's, but if the challenge is worth it to you, you simply may need to mostly figure things out on your own.

(Apr 7, 2023 08:48 AM)iCasher Wrote: [\[CITE\]](#) - build your payload , encrypt it from AV's

- build fake page to SE your victims
- edit your dns to redirect all the network users to your fake download page before they go to anywebsite
- wait your victims

this is very basic and most effective way to infect other PC's on the same lan , ofc there are vulnerability's you can use and long way for checking open ports on each machine or running services etc but i suggest you the first option

You forgot to add the important disclaimer that DNS spoofing only works on non-HSTS websites.