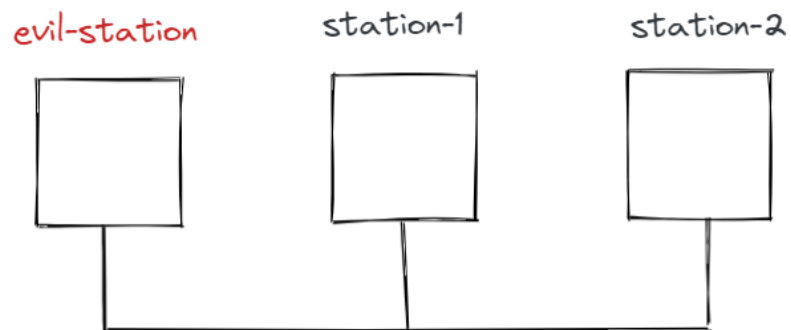


LAB 1

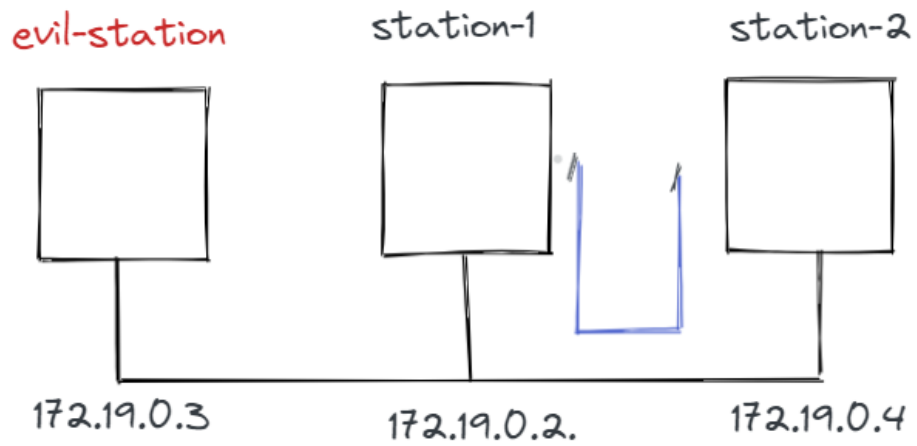
Upoznali smo se s osnovnim sigurnosnim prijetnjama i ranjivostima u računalnim mrežama. Analizirali smo ranjivost Address Resolution Protocol-a (ARP) koja napadaču omogućava izvođenje man in the middle i denial of service napada na računala koja dijele zajedničku lokalnu mrežu (LAN).



Nakon što smo ustanovili da su na istoj lokalnoj mreži(tako što smo pronašli MAC adrese), uspostavili smo komunikaciju između station-1 i station-2.

station-2 netcat -l -p 8080

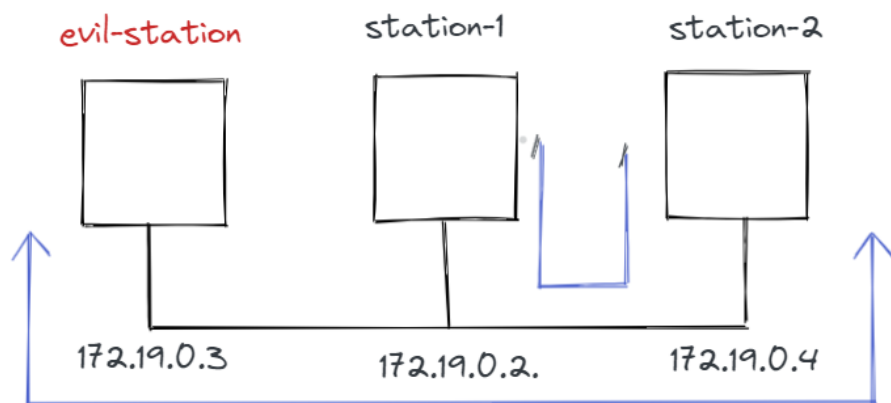
station-1 netcat station-2 8080



Zatim želimo da evil-station može presresti poruku, odnosno vidjeti njen sadržaj.

arp spoof [-t target][-r] host

U našem slučaju je target station-1, a host station-2.



source	destination	IP	IP	data
	evil-station	evil-station	station-2	

Objašnjenje slike iz uputa za lab1(zašto piše IP od evil-station, a ne IP od station-1 ili station-2)

Za kraj smo pokušali station-2 isključiti iz komunikacije. Odnosno vidjeti sve što station-2 šalje station-1, a ono što station-1 šalje vidi samo evil-station.

tcpdump-X host station-1 and not arp

echo 0> /proc/sys/net/ipv4/ip_forwarddot@

OVO JE PRIMJER AKTIVNOG NAPADA

Sara Ćurak

računarstvo 120