NeverLAN CTF

PCAP : hidden-ctf-on-my-network

Value : 250 pts

Difficulty : Unknown

Description : So, I have a little CTF challenge I’ve been running on my home network for about a year now. No one has noticed it and i doubt anyone ever will… Until today !

I grabbed a hak5 plunderbug and recorded the trafic of a cheap HP machine booting up for the first time on my network. Can you solve the CTF challenge I leave for my guests ?

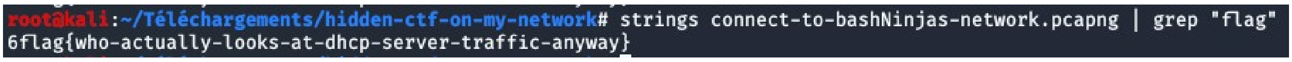
Attachment : hidden-ctf-on-my-network.7z

Solution :

First download the attachment «hidden-ctf-on-my-network.7z» and extract his content. We found a Readme.md file, with the same description of the challenge with «Wireshark ?» as tittle. With our challenge file «connect-to-bashNinjas-network.pcapng».

Unintended way :

I was able to extract the flag with a grep command after reading the file with «strings».

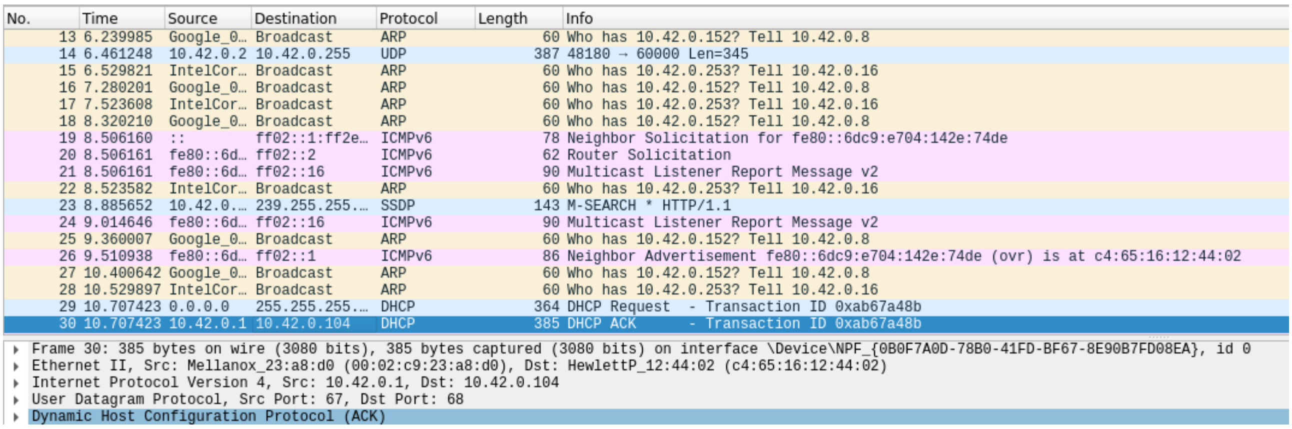


```
root@kali:~/Téléchargements/hidden-ctf-on-my-network# strings connect-to-bashNinjas-network.pcapng | grep "flag"
6flag{who-actually-looks-at-dhcp-server-traffic-anyway}
```

Flag : flag{who-actually-looks-at-dhcp-server-traffic-anyway}

Intended way (via Wireshark) :

First we will open the pcapng file with wireshark.

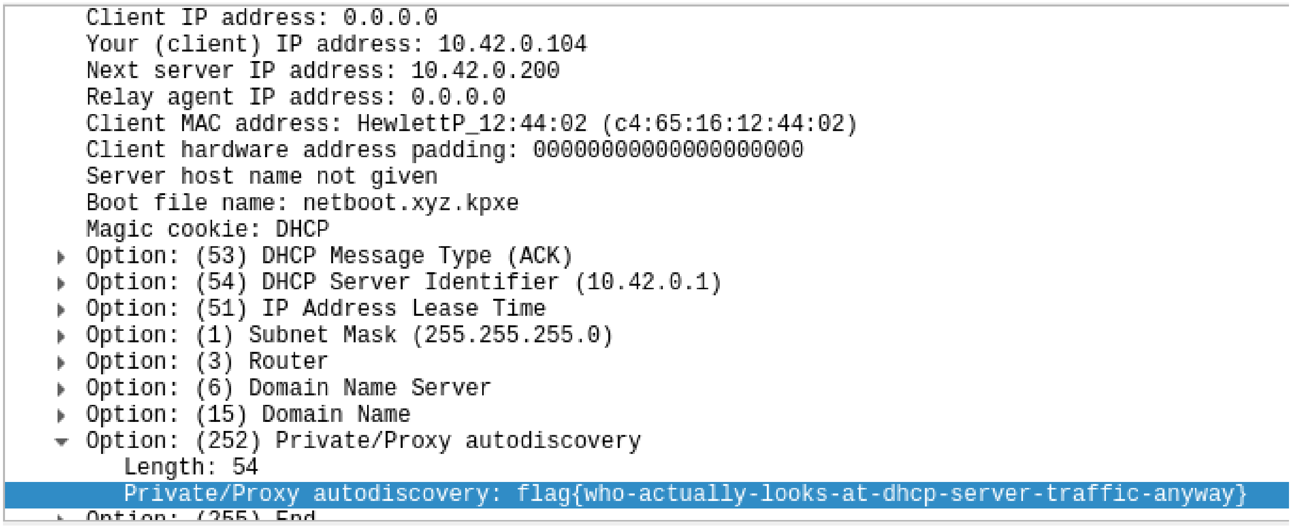


```
No.       Time      Source     Destination    Protocol     Length  Info
      13 6.239985  Google_0… Broadcast      ARP            60 Who has 10.42.0.152? Tell 10.42.0.8
      14 6.461248  10.42.0.2 10.42.0.255    UDP           387 48180 → 60000 Len=345
      15 6.529821  IntelCor… Broadcast      ARP            60 Who has 10.42.0.253? Tell 10.42.0.16
      16 7.280201  Google_0… Broadcast      ARP            60 Who has 10.42.0.152? Tell 10.42.0.8
      17 7.523608  IntelCor… Broadcast      ARP            60 Who has 10.42.0.253? Tell 10.42.0.16
      18 8.320210  Google_0… Broadcast      ARP            60 Who has 10.42.0.152? Tell 10.42.0.8
      19 8.506160  ::        ff02::1:ff2e…  ICMPv6         78 Neighbor Solicitation for fe80::6dc9:e704:142e:74de
      20 8.506161  fe80::6d… ff02::2        ICMPv6         62 Router Solicitation
      21 8.506161  fe80::6d… ff02::16       ICMPv6         90 Multicast Listener Report Message v2
      22 8.523582  IntelCor… Broadcast      ARP            60 Who has 10.42.0.253? Tell 10.42.0.16
      23 8.885652  10.42.0.… 239.255.255.…  SSDP          143 M-SEARCH * HTTP/1.1
      24 9.014646  fe80::6d… ff02::16       ICMPv6         90 Multicast Listener Report Message v2
      25 9.360007  Google_0… Broadcast      ARP            60 Who has 10.42.0.152? Tell 10.42.0.8
      26 9.510938  fe80::6d… ff02::1        ICMPv6         86 Neighbor Advertisement fe80::6dc9:e704:142e:74de (ovr) is at c4:65:16:12:44:02
      27 10.400642 Google_0… Broadcast      ARP            60 Who has 10.42.0.152? Tell 10.42.0.8
      28 10.529897 IntelCor… Broadcast      ARP            60 Who has 10.42.0.253? Tell 10.42.0.16
      29 10.707423 0.0.0.0   255.255.255.…  DHCP          364 DHCP Request  - Transaction ID 0xab67a48b
      30 10.707423 10.42.0.1 10.42.0.104    DHCP          385 DHCP ACK      - Transaction ID 0xab67a48b

 ▸ Frame 30: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits) on interface \Device\NPF_{0B0F7A0D-78B0-41FD-BF67-8E90B7FD08EA}, id 0
 ▸ Ethernet II, Src: Mellanox_23:a8:d0 (00:02:c9:23:a8:d0), Dst: HewlettP_12:44:02 (c4:65:16:12:44:02)
 ▸ Internet Protocol Version 4, Src: 10.42.0.1, Dst: 10.42.0.104
 ▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
 ▸ Dynamic Host Configuration Protocol (ACK)
```

As i was spoiled by the flag with my uninteded way, i looked as the DHCP request.

Analyzing the DHCP request, we can see the flag inside the «Private / Proxy autodiscovery» option.



```
      Client IP address: 0.0.0.0
      Your (client) IP address: 10.42.0.104
      Next server IP address: 10.42.0.200
      Relay agent IP address: 0.0.0.0
      Client MAC address: HewlettP_12:44:02 (c4:65:16:12:44:02)
      Client hardware address padding: 00000000000000000000
      Server host name not given
      Boot file name: netboot.xyz.kpxe
      Magic cookie: DHCP
    ▸ Option: (53) DHCP Message Type (ACK)
    ▸ Option: (54) DHCP Server Identifier (10.42.0.1)
    ▸ Option: (51) IP Address Lease Time
    ▸ Option: (1) Subnet Mask (255.255.255.0)
    ▸ Option: (3) Router
    ▸ Option: (6) Domain Name Server
    ▸ Option: (15) Domain Name
    ▾ Option: (252) Private/Proxy autodiscovery
         Length: 54
         Private/Proxy autodiscovery: flag{who-actually-looks-at-dhcp-server-traffic-anyway}
    ▸ Option: (255) End
```

Flag : flag{who-actually-looks-at-dhcp-server-traffic-anyway}