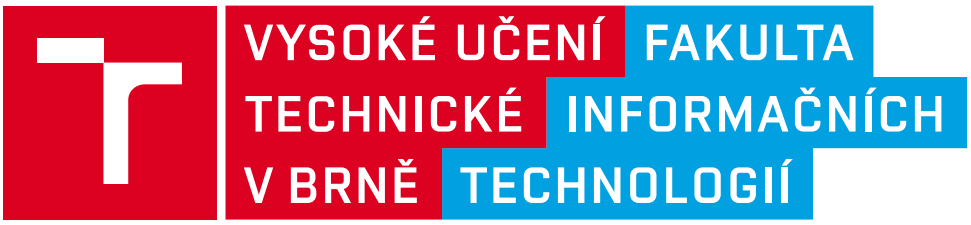
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií



Computer Communications and Networks 2017/2018

Project n. 2, variant 2 (DHCP Starvation attack)

Erik Kelemen *xkelem01*

April 9, 2018

Introduction

DHCP Starvation attack has two well-known variants, main idea behind first is sending tons of DHCP DISCOVER messages and not replying to DHCP OFFERs, which keeps DHCP server busy unabled to respond valid clients requests. Second variant is about simulating valid ip requests, which gradualy exhaust ip pool. So DHCP server has no more ip addresses to offer. I attempted to implement both variants.

Implementation

My solution required implementation of raw socket from layer 2 (Ethernet frame), building up to application layer manually. Reason for that was need of simulate fake MAC address as Ethernet source MAC address. With mentioned precaution DHCP starvation attack will leave less trails. As third layer I chose IPv4 and above there is UDP as application layer. UDP is strictly set on ports 67 and 68 as DHCP protocol requires according to RFC 2131. Data were filled with DHCP messages, tricky part about it was various length of option field. I solved it with static length, ending with octet '255' reffering end of options and space between valid options and end I filled with octets '0' reffering padding. First problem occured when DHCP DISCOVER message with fake MAC address was sent and DHCP server was trying to sent unicast to this false address(which is not ours, or even may not exists). I solved it with broadcast flag, asking server to reply DHCP OFFER as broadcast. Also this is one of restrictions of my solution, because even if broadcast flag is set, server can still decide to refuse it and send unicast. Although, hopefuly we overcome this succesfuly as next step we reply with DHCP REQUEST. This is how one IP address is stolen from pool. Repeating provide loop, which has implemented breaking mechanism similiar to watchdog. In simple words: "break the loop if you failed five times in row". After this condition we assume that whole IP pool was stolen and attack is done.

Testing

Network Topology

I composed Network from router model - zyxel NBG-416N (representing DHCP server) my laptop (attacker) and mobile device(victim)

Test results

Firstly I tried it through wi-fi. I encountered restrictions which blocked my attempts to send packets from false MAC address, so I switched to ethernet. After that, everything worked. When IP pool was exhausted I tried to connect to network with mobile device. It stopped at status 'Načítávaní IP adresy' as expected.