Project Title: ICMP SMURF ATTACK

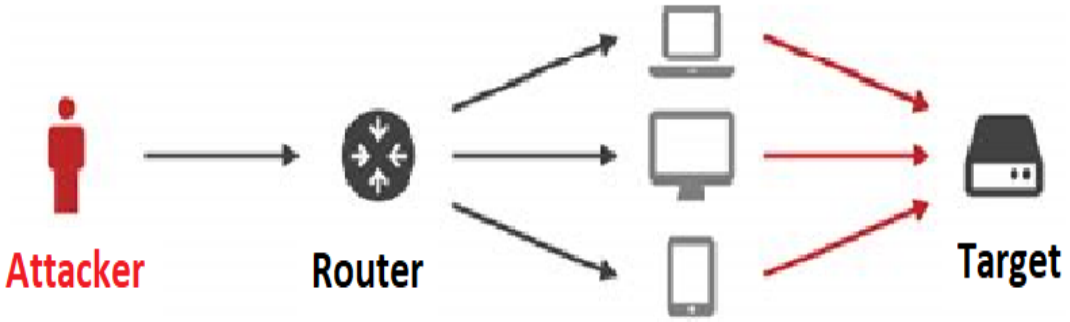
Name: Akid Abrar
ID: 1605100

ICMP SMURF ATTACK:

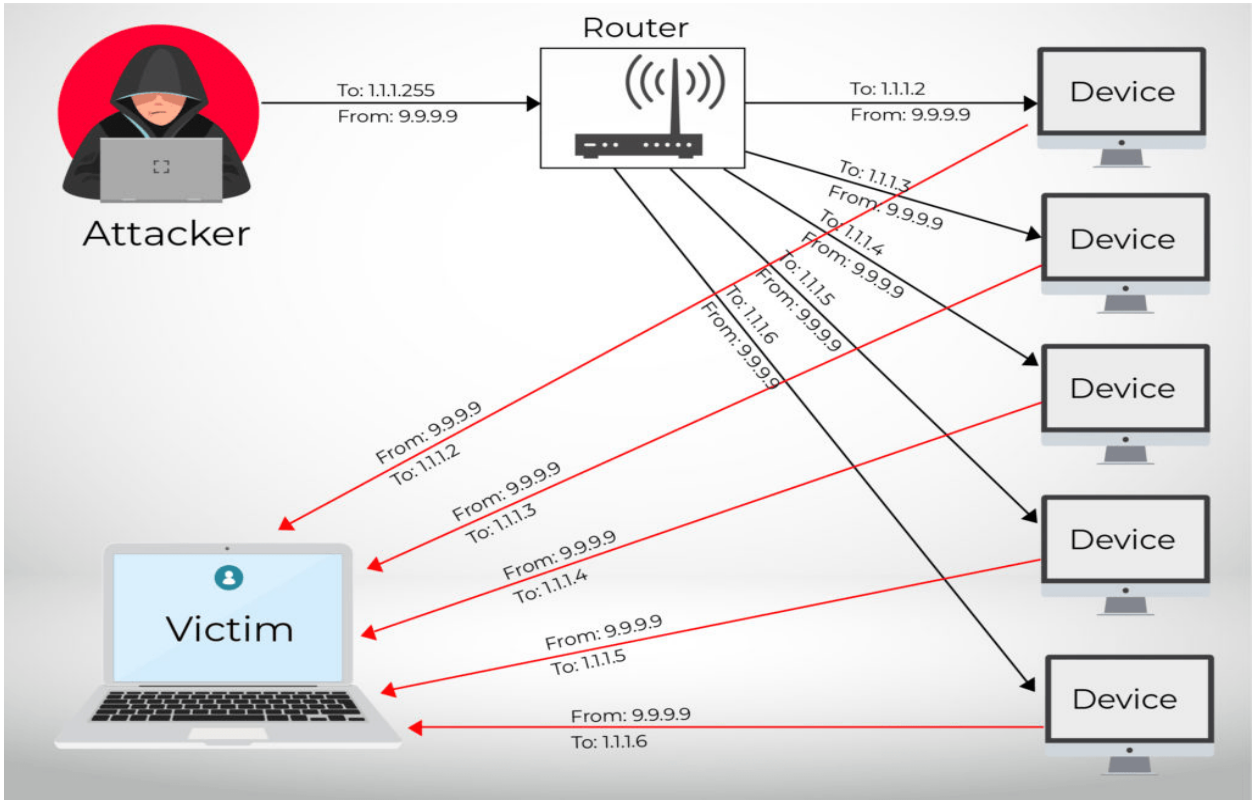
ICMP smurf attack is an DoS attack where a malicious attacker will trigger a large number of ICMP echo messages to one or more destinations with the target victim's spoofed address as the source IP address of the ICMP echo messages. This will result in the victim host receiving a large volume of echo reply messages, causing its buffer to overrun or fill the available bandwidth of the victim to make it unable to connect with other users.

To generate a large number of echo reply msg,the attacker send the ICMP echo request message with spoofed Source IP to the broadcast address of the Router.When a Router receives any packet in its broadcast address,all the devices connected to Router get the packet.After receiving the echo message with victim’s Source IP spoofed in it,all the devices send echo reply message to the victim’s IP.Receiving this huge number of message,the victim becomes slow or unavailable for a while.

TOPOLOGY DIAGRAM:

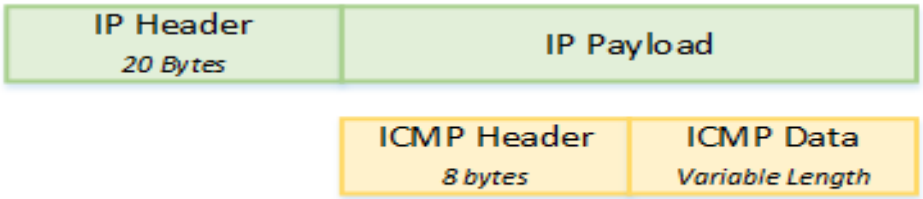


TIMING DIAGRAM:

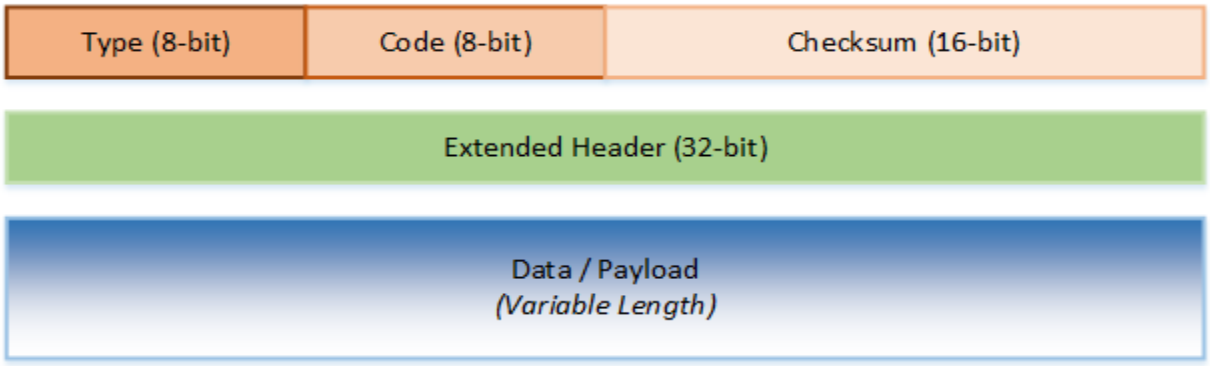


ICMP PACKET DETAILS:

It has 20 bytes of Header and Variable length ICMP message with 8 bytes of ICMP Header.Here, the last 4 bytes of the ICMP Header is generally not used.



Below shows the format of an ICMP message. There are different values for the type field, which identify the ICMP message. So a type of ICMP message will use different values of the code field to specify the condition.



The last field talks about the Checksum. Before an ICMP message is transmitted, the checksum is computed and is inserted into the field. So at the receiving end the checksum is calculated again and verified against the checksum field. If any mismatch is found, then it confirms that an error or change has occurred.And the last 4 bytes are normally not used.

DESIGN STRATEGY:

I have to construct ICMP Packet in attacker's PC according to the above described structure.I will use 1 virtual machine as attacker,1 as victim and 3 others to implement the attack. I can find find the victim's IP address by ipconfig command.Then the attacker virtual machine will send ICMP_ECHO REQUEST to all other machines containing the victim's IP as the source IP.The other machines will reply back ICMP_ECHO REPLY to the victim's machine,we'll check these replies in victim's PC using wireshark.

JUSTIFICATION:

The main goal of the attack is achieved in this design,as 3 virtual machines will send ICMP_ECHO REPLY to victim's machine without knowing that they are working as Sa part of an attack.