|  |  |  |
| --- | --- | --- |
| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | Assignment No:01 |
| Section: B | Date: 27/08/2022 |

|  |  |
| --- | --- |
| Task 1.1 A | Sniff IP packets using Scapy. |
| Output Screenshot | From Host-A:    Pinging from Host-A to 8.8.8.8 ([www.google.com](http://www.google.com)) 12 packets transmitted.  On Attacker Terminal:    Observation:  A packet received which has 4 headers like Ethernet, IP, ICMP, Raw.  ICMP packets received on attacker’s terminal after Pinging from host-A IP:10.9.0.5  Type of IP address is IPv4 and checksum of IP header is also calculated as 0x6dla  ICMP packet checksum is 0x2ad7, Raw packet load is present in some encrypted format. |
| Task 1.1 B | Capture only the ICMP packet |
| Output Screenshot | From Host A:    Pinging from Host-A to 8.8.8.8 ([www.google.com](http://www.google.com)) 5 packets transmitted.  On Attacker Terminal:    Observation:  A packet received which has 4 headers like Ethernet, IP, ICMP, Raw.  Only ICMP packet received on attacker’s terminal after pinging from host-A IP:10.9.0.5 by using filter  Type of IP address is IPv4 and checksum of IP header is calculated as 0x4466  ICMP packet echo-request checksum is 0x98dc, sequence no 1.  Raw packet load is present in some encrypted format |
| Q) | Capture any TCP packet that comes from a particular IP and with a destination port number 23 |
| Output Screenshot | From Host A:  Connecting with telnet from IP address 10.9.0.1.  Got login portal sign in successfully and got connected to successfully.  Now terminating the telnet connection.    On Attacker Terminal:    Observation:  When host-A was trying to connect with talent service then TCP packet received.  Here packet received which has only 4 headers like Ethernet, IP, TCP.  Only TCP packet received on attacker’s terminal after establishing connection from host-A IP:10.9.0.5 by using filter.  Type of IP address is IPv4 and checksum of IP header is calculated as 0x6bae  TCP packet dport is telnet and checksum is ox1446, ack is 0, Note here RAW packet is not Present |
| Q) | Capture packets that come from or go to a particular subnet |
| Output Screenshot | From Host A    Pinging from Host-A to IP 172.17.0.1 which is in same subnet, ping successful sending a sequence of ICMP Packet.  8 packet successfully transmitted in time 7152ms.  On Attacker Terminal:    Observation:  A packet received which has 4 headers like Ethernet, IP, ICMP, Raw.  Type of IP address is IPv4 and checksum of IP header is calculated as 0xb7e3, in same subnet  ICMP packet echo-request checksum is 0x84ad, sequence no 0x1.  Raw packet load is present in some encrypted format. |
| Task 1.2 | spoofing ICMP echo request packets |
| Output Screenshot | On Attacker Terminal:    Observation:  Sending a spoofed packet from source=10.9.0.1 to destination=10.9.1.5  Photocall type ICMP, IP address is type is IPv4  NOTE: checksum is None it will be considered as missing checksum but will be allowed and flags field is also empty length of packet is not defined. And tos is 0x0.  Wireshark:    For ICMP Echo request from 10.9.0.1 we got an ICMP Echo reply from 10.9.0.5 |
| Q.) | spoofing ICMP echo request packets arbitrary source IP address |
| Output Screenshot | On Attacker Terminal:    Observation:  Similar to above here we are spoofing to arbitrator IP address as you can see that in ICPM header code, checksum, id, sequence everything is 0.  We send only IP, ICMP header part rest all is set to default value by scapy module.  ttl value is 64 so packet was not able to reach to destination and IP version is IPv4, flags are not set  Wireshark:    As you can that see sending packet to arbitrary address is we are unable to receive Echo reply packet. While we tried to send ICMP packet 3 times but no rely was found. |
| Task 1.3: | Traceroute |
| Output Screenshot | On Attacker Terminal    Observation:  As you can see that when we try to trace the packet of IP 157.240.23.35 it went to 4 hops and then connection closed, possible cause might be that IP doesn’t exist.  Wireshark:  When we try to ping the destination of packet length 72 byes time to live was exceeded that indicates that IP is currently not reachable. |
| Task 1.4 | Sniffing and-then Spoofing |
| Output Screenshot | From Host A:    Host-A trying to ping a non-existing IP address 1.2.3.4 and still getting response message.  10 packets transmitted and 10 packet received.  On Attacker Terminal:    Observation:  When the Host-A try to ping some imaginary IP address our program sniff that packet and create an Echo-reply packet with the source address of that imaginary IP address and send back to host-A.  Wireshark:    ICMP Echo request message was sent by the Source 10.9.0.5 to destination 1.2.3.4 even the destination doesn’t exist but we can see that ICMP ECHO reply message is send from 1.2.3.4 to host-A which is clearly a spoofed packet. |

THANKING YOU