Experiment 6

Chinmay Parikh A059

Questions

1. What is IP spoofing?
2. Is IPSec helpful in preventing IP Spoofing? Explain in detail.
3. What are other counter measures available for IP spoofing?
4. List the features of engage packet builder.
5. List the features of Wireshark.

Answers

1. IP spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. It causes serious security problem in the cyber world, and is currently exploited widely in the information warfare.

2. IPsec is a security mechanism that provides peer-entity authentication, data-origin authentication, data integrity, and optionally data confidentiality. It relies on extensions to the standard IP header layout and an additional protocol. The security services that IPSec can provide are:

   - Authorization–access control
   - Connectionless data integrity;
   - Data-origin authentication;
   - Peer-entity authentication;
   - Rejection of replayed packets;
   - Confidentiality (encryption); and
   - Limited traffic flow confidentiality.

3.

4. Engage Packet builder is a powerful and scriptable packet builder for Windows platform. The program features: packet injection starting from link layer (MAC address spoofing), supporting following transport protocols (TCP, UDP, ICMP), custom payload in hex format / ASCII format, ASCII to Hex converted built-in, scripting engine, great for Firewall and IDS testing, SYN-Floods can be generated very easy, build “strange” packets (SYN-FIN forexample) and full control over sequence and acknowledge number, window size and urgent pointer. Packet injection starting from link layer (MAC address spoofing), supporting following transport protocols:

Threat	Countermeasures
Spoofing user identity	Use strong authentication. Do not store secrets (for example, passwords) in plaintext. Do not pass credentials in plaintext over the wire. Protect authentication cookies with Secure Sockets Layer (SSL).
Tampering with data	Use data hashing and signing. Use digital signatures. Use strong authorization. Use tamper-resistant protocols across communication links. Secure communication links with protocols that provide message integrity.
Repudiation	Create secure audit trails. Use digital signatures.
Information disclosure	Use strong authorization. Use strong encryption. Secure communication links with protocols that provide message confidentiality. Do not store secrets (for example, passwords) in plaintext.
Denial of service	Use resource and bandwidth throttling techniques. Validate and filter input.
Elevation of privilege	Follow the principle of least privilege and use least privileged service accounts.

- TCP (RFC 793)
- UDP (RFC 768)
- ICMP (RFC 792)

5. Wireshark is software that “understands” the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports. Data can be captured “from the wire” from a live network connection or read from a file of already-captured packets. Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback. Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark. Captured files can be programmatically edited or converted via command-line switches to the “editcap” program. Data display can be refined using a display filter. Plug-ins can be created for dissecting new protocols. VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played. Raw USB traffic can also be captured.