chapter - 11

Session Hijacking

Concepts

- absence of invalid session ids
- indefinite session timeout
- weak session id generation algorithm.
- insecure handling of session IDs
- without encryption, countermeasure won't work.

Process

1. Sniff (MITM)
2. Monitor (predict sequence no.)
3. Session desyncronisation (break connection)
4. Session ID prediction (take over id)
5. command Injection. (inject packets)

Types

Active (hijacks, seizes, control)

Passive (hijacks, watch, record, gather)

OSI Model

Network (Interception of Packets TCP/UDP)

Application (gain control — HTTP User session)

Application level Hijacking

- Session token is stolen / predicted

Session Sniffing

MITM attack

XSS attack

Session replay attack

CRIME attack.

Predictable session ID

MITB attack (trojan)

Cross site request forgery

Session Fixation

Forbidden attack

Session donation attack

CRIME attack

- Compression Ratio Info Leak Made Easy
- exploits vulnerabilities in data compression
- hijacks by decrypting session cookies

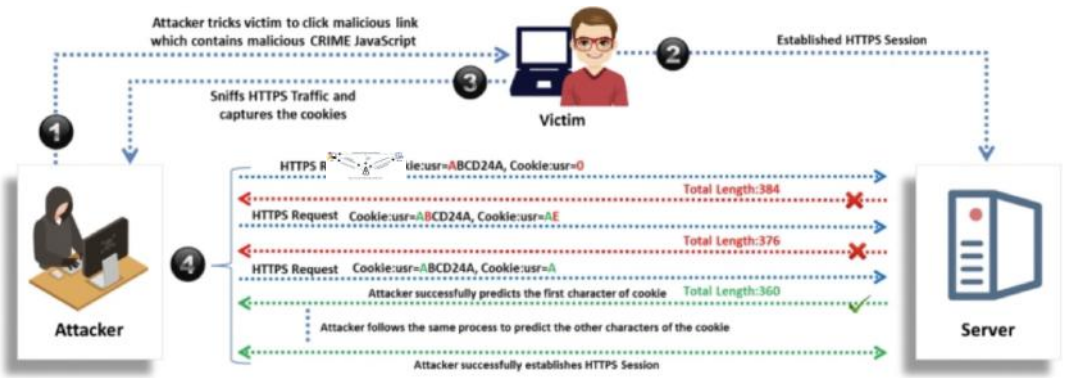

Figure 11.18: Session hijacking using a CRIME attack

Forbidden Attack

- a type of MITM attack.
- hijacks HTTPS sessions.
- uses reuse of cryptographic nonce.

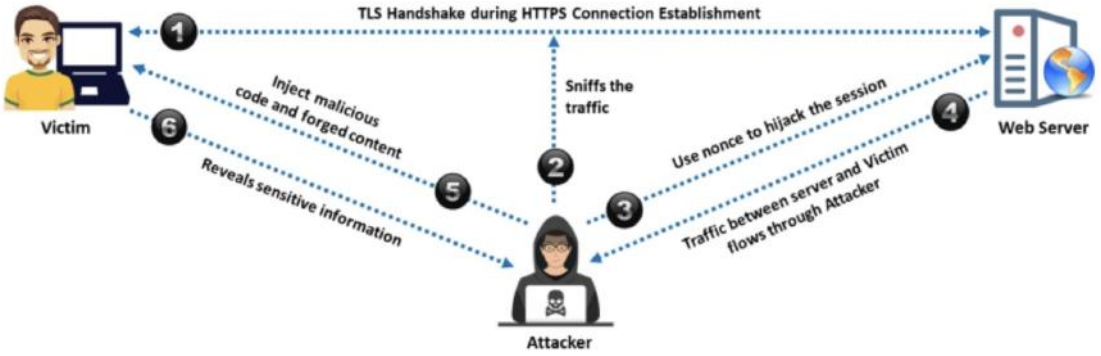

Figure 11.19: Session hijacking using a forbidden attack

Donation attack

- donates session ID to target user,
- victim clicks the link and login account

Network level Hijacking

Blink Hijacking

UDP "

TCP/IP " ✓

RST Hijacking ✓

MITM - Packet

IP Spoofing - Source

TCP/IP Hijacking

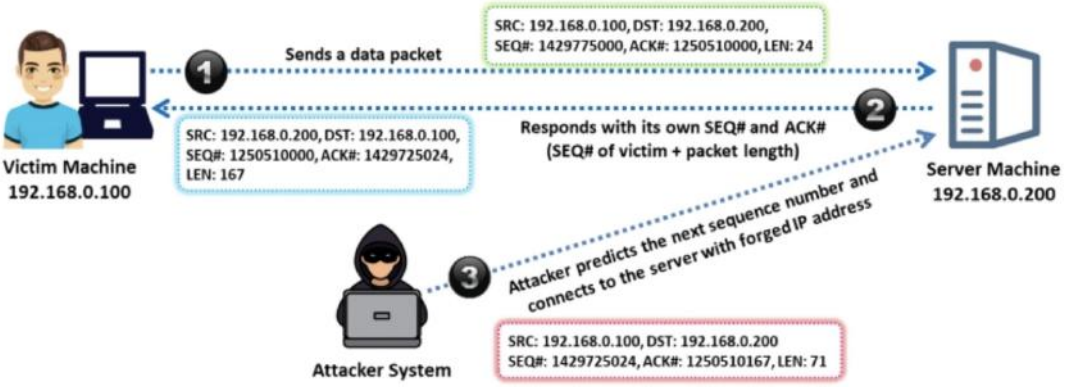

Figure 11.22: TCP/IP hijacking process

RST Hijacking

- injects authentic RST Packet Using Spoof ID & Predicted Ack
- attacker resets connection for victim.

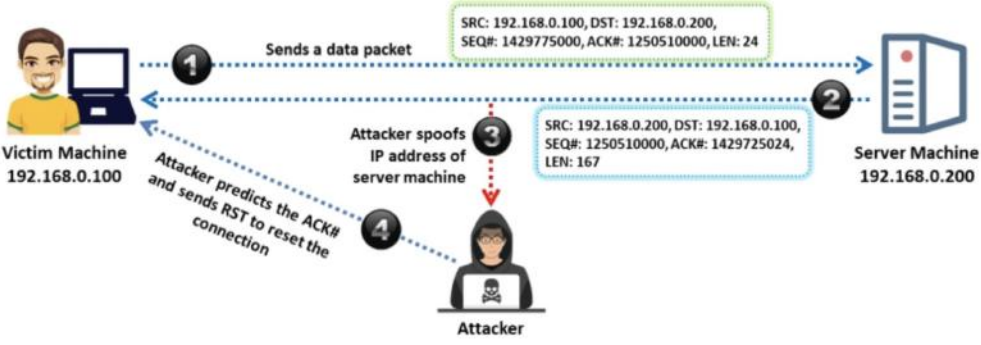

Figure 11.23: RST hijacking process

Tools:

- Burp Suite
- Droid Sheep
- Droid Sniff
- FaceNiff
- Cx SAST
- Fiddler

Prevention:

- HTTP strict Transport Security. (Policy)
- Token binding.
- HTTP public key pinning.
- VPN (encrypted tunnel)
- 2FA