Network & Web Security

1 Border Gateway Protocol

- What if you want to take down a big chunk (or all) of the internet
- BGP trusts all route announcements sent by its peers
- Announcing a shorter route through a blank page would cause chaos

2 Router Security

Security Features:

- Firewalls (also stateful packet inspection)
- VPN Handling
    - Confidentiality via encryption
    - Authentication
    - Message integrity (detect instances of tampering with transmitted messages)

NAT

- Allows a LAN to appear under a single machine with a single IP address (e.g. limited IPv4 address space)
- Breaks the end to end communication model
- NATs don't make internal network topology secure

3 Telnet, SSH, Netcat and FTP

- Telnet is a very old protocol that should not be used any more
    - All data is sent unencrypted in plain text
    - Easy to capture passwords using a packet sniffer
    - Subject to MITM attacks
- Telnet replaced by SSH
    - Strong encryption with public key authentication ensuring remote computer is who it claims to be
- FTP is also obsolete (except insensitive data)
    - Sends login and password in clear text vulnerable to sniffing attacks
    - Do FTP over SSH (SFTP)
    - Check FTP server path is pointing to sensible location

4 ARP Vulnerabilities and NDP

- Maps Internet Protocol (IPv4, 32bits) address to physical machine (MAC address, 48bits)
- Vulnerable to
    - ARP Spoofing
        * Steal sensitive information
        * DoS, MITM, Session-Hijacking
    - MAC Flooding
    - MAC Duplicating
- Still widely used, but replaced by NDP for IPv6

5 NDP

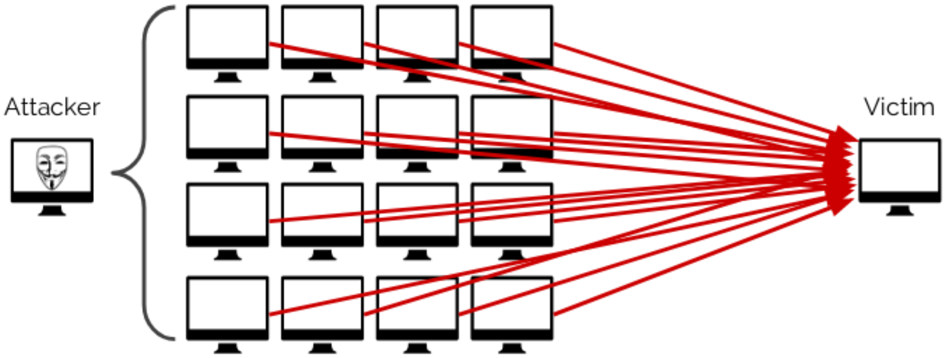
- Also resolved network layer (IP) and link layer like ARP, but for IPv6
- Secure Neighbour Discovery (SEND) security extension
  - Cryptographically generated addresses ensure that the claimed source of an NDP message is the owner of the claimed address
- Offers lots of improvements over IPv4 equivalent protocols. Some:
  - Better router discovery
  - More robust to failures where neighbours become unreachable
- But still far from perfect
  - Still vulnerable to MITM via:
    - Spoofed ICMPv6 neighbourhood router advertisement
    - Rogue DHCPv6 Servers, and other approaches
  - Vulnerable to DoS by flooding and many others

6 IP Spoofing

- Changing the source IP of a packet with a fake IP address to hide the identify of the sender
- The victim thinks he's talking to his friend, but actually he's talking to the hacker
- Protection
  - Authentication protocol
  - Encrypted sessions
  - Access control lists (ACLs)
  - Filtering of traffic
  - Proper router configuration

7 Distributed Denial of Service (DDoS)

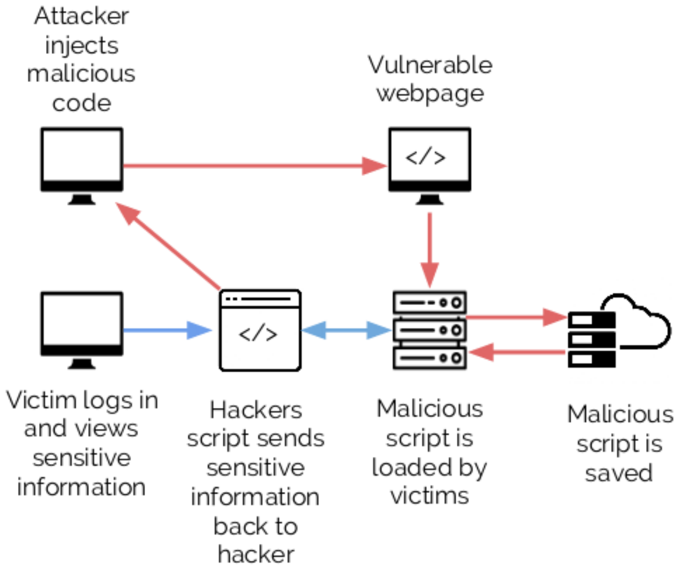
This is very difficult to protect against



8 Wiretapping

A passive splice tap can be placed in a copper cable in order to read all the data passing along the cable

9 Cross-Site Scripting (XSS)


Attacker injects malicious code
Vulnerable webpage
</>
</>
Victim logs in and views sensitive information
Hackers script sends sensitive information back to hacker
Malicious script is loaded by victims
Malicious script is saved

Protection

- Whitelisting - only allow valid inputs on server
- HTML escaping
- Sanitization
- Blacklisting - quite fragile and not very good

10 Cookies

Credential tokens:

- Held in local browsing session
- Identify you to a remote web server
- Remember states
  - Shopping cart
  - Browsing history
  - Data in form fields
- Common target for hackers