CSE 40567 / 60567: Computer Security

Network Security 4
Homework #6 has been released. It is due Tonight at 11:59PM

See Assignments Page on the course website for details
Guest Lecture 4/11: Mike Schiffman, Salesforce Threat Intelligence Team
Covert Channels
Overt vs. Covert Secure Channels

**IPSEC is an overt protection mechanism**

<table>
<thead>
<tr>
<th>IP header</th>
<th>ESP</th>
<th>Encapsulated IP packet or TCP header + payload</th>
<th>ESP</th>
</tr>
</thead>
</table>

**Covert channels hide data in a non-obvious way**

| IP header | ? | TCP Header | ? | Payload | ? |
Many places to squirrel away data

**IP Header**

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Bits</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>4</td>
<td>Protocol version</td>
</tr>
<tr>
<td>IHL</td>
<td>4</td>
<td>Internet Header Length</td>
</tr>
<tr>
<td>Type of Service</td>
<td>8</td>
<td>Type of service</td>
</tr>
<tr>
<td>Total Length</td>
<td>16</td>
<td>Total length of IP header</td>
</tr>
<tr>
<td>Identification</td>
<td>13</td>
<td>Identification</td>
</tr>
<tr>
<td>Flags</td>
<td>4</td>
<td>Flags</td>
</tr>
<tr>
<td>Fragment Offset</td>
<td>13</td>
<td>Fragment offset</td>
</tr>
<tr>
<td>Time to Live</td>
<td>8</td>
<td>Time to live</td>
</tr>
<tr>
<td>Protocol</td>
<td>8</td>
<td>Protocol used</td>
</tr>
<tr>
<td>Header Checksum</td>
<td>16</td>
<td>Header checksum</td>
</tr>
<tr>
<td>Source Address</td>
<td>32</td>
<td>Source IP address</td>
</tr>
<tr>
<td>Destination Address</td>
<td>32</td>
<td>Destination IP address</td>
</tr>
<tr>
<td>Options</td>
<td>0-64</td>
<td>Options</td>
</tr>
<tr>
<td>Data</td>
<td>0-65535</td>
<td>Data</td>
</tr>
</tbody>
</table>
```

20 Bytes
Many places to squirrel away data

TCP Header

<table>
<thead>
<tr>
<th>Data Offset</th>
<th>Reserved</th>
<th>URG</th>
<th>ACK</th>
<th>PSH</th>
<th>RST</th>
<th>SYN</th>
<th>FIN</th>
<th>Window Size</th>
<th>Checksum</th>
<th>Urgent Pointer</th>
<th>Options</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Many places to squirrel away data

Create a tunnel with ping requests and responses

<table>
<thead>
<tr>
<th>8-bit ICMP Type</th>
<th>8-bit ICMP Code</th>
<th>16-bit ICMP Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ICMP Contents (dependent on type and code)</td>
</tr>
</tbody>
</table>
Many places to squirrel away data
Steganography
Timing channels

Convey information by triggering or delaying events at set time intervals
Frequency-based channels

Convey information by triggering or delaying events at set time intervals

The ordering or combination of cover channel activity encodes the secret
Software packages

Tunnelshell: https://packetstormsecurity.com/search/files/?q=Tunnelshell

RECUB: http://mir-os.sourceforge.net/recub.htm

ptunnel: http://www.mit.edu/afs.new/sipb/user/golem/tmp/ptunnel-0.61.orig/web/

dns2tcp: in apt
Distributed Denial of Service Attacks
Botnets
Distributed Denial of Service Attacks

1. How a botnet works
2. OK
3. 3
4. How a botnet works
What does DDoS traffic look like?

General strategy: blast target with as many packets as possible

- Saturates bandwidth
- May crash OS

- Flood attacks
- Amplification attacks
- Resource depletion attacks

S. Specht and R. Lee, “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures”, 2004
Flood Attacks

**UDP Flood Attack**

- Victim
- 12.3.66.101
- 128.11.231.17
- 128.9.21.11
- 99.41.200.58
- UDP 10
- UDP 11
- UDP 12
- UDP 65,535

**ICMP Flood Attack**

- Victim
- 12.3.66.101
- 128.11.231.17
- 128.9.21.11
- 99.41.200.58
- ICMP Echo Requests / ICMP Echo Responses
Amplification Attacks

Attacker with 1Mbps

10 compromised triggers

1Mbps Connection

1Gbps connection x10

400 amplifier machines

Amplification factor of 50x

500Gbps from amplifiers hits victim

Resource Depletion Attacks

1. TCP SYN Attack

Attacker \(\rightarrow\) Web Server

- SYN
- SYN-ACK
- SYN
- SYN-ACK

Send SYNs until no more connections can be established

2. TCP PSH + ACK Attack

Attacker \(\rightarrow\) Web Server

- PSH + ACK
- ACK
- PSH + ACK
- ACK

Send PSH + ACKs until target’s resources are exhausted
Insidious: direct lots of legitimate traffic to site

https://twitter.com/search?q=%22RIP%20Paul%20McCartney%22

[REDACTED] @Snurbed · Jan 15
RIP Paul McCartney, you changed the world with your music and you’ll never be forgotten #FarewellPaul

TCP SYNs

paulmccartney.com
Defenses

• Attacks on the decline (?)
  ‣ Reported peak in the early to mid-2000s (Kaspersky Lab)

• Technical countermeasures are now commonplace
  ‣ Firewalls
  ‣ Switches with rate-limiting and ACLs
  ‣ Routers with rate-limiting and ACLs

Botnet DDoS Attacks: Q4 2015

Kaspersky Lab Report

• Resources in 69 countries were targeted by DDoS attacks.
• 94.9% of the targeted resources were located in 10 countries.
• Largest numbers of DDoS attacks targeted victims in China, the US and South Korea.
• Longest DDoS attack lasted for 371 hours (or 15.5 days).
• SYN DDoS, TCP DDoS and HTTP DDoS remain the most common attack scenarios.
• The proportion of DDoS attacks from Linux-based botnets was 54.8%.