Lecture 27: Network Security

CS 105
Networking Stack

1 - Physical
   - Deliver signals

2 - Data Link
   - Deliver locally

3 - Network
   - Deliver globally

4 - Transport
   - Deliver (un)reliably

5 - Session
   - Manage sessions

6 - Presentation
   - Manage encoding

7 - Application
   - Deliver content

HTTP
   - Deliver content

TLS/SSL
   - Manage encoding

TCP/UDP
   - Manage sessions

IP
   - Deliver (un)reliably

Ethernet
   - Deliver globally

0s and 1s
   - Deliver locally
Denial of Service Attacks

- Goal: violate availability by making system unable to respond to requests from legitimate users
  1. Resource-saturation attacks
  2. Vulnerability-based attacks
Ping

- The **Internet Control Message Protocol (ICMP)** is a network-layer support protocol used to pass operational information and error messages.

- **ping**: test reachability of a host in an IP network
  - sends ICMP echo request packet to target host and waits for ICMP echo reply
  - Uses CPU, network bandwidth

- **traceroute**: display path to a host in an IP network
Ping Flood

- ping -f
Ping Flood
Defenses against Ping Floods

- Disable ICMP functionality
- Non-centralized firewalls
DNS Flood
TCP

• Reliable
  • acknowledgement
  • checksum
  • sequence number

• In-order
  • sequence number

• Congestion control
  • slow start
  • congestion avoidance
  • fast retransmit
  • fast recovery
SYN Flood

Attacker

Bot

Spoofed SYN Packet

Spoofed SYN Packet

Target

SYN-ACK

SYN-ACK

SYN-ACK

SYN-ACK

SYN-ACK
Defending Against SYN Floods

- Increase RECV queue size
  - Attackers might have enough resources to fill

- Recycle oldest half-open connections
  - What happens if the attacker quickly sends a lot of syns?

- SYN cookies
  - No longer storing a queue of connections
DNS Reflection Attacks
DDOS Attacks
Mitigating DoS Attacks
## Mitigating DoS Attacks

<table>
<thead>
<tr>
<th></th>
<th>Gold Award</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application Firewall</td>
<td>?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Rate Limiting</td>
<td>?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Automatic Bot Discernment</td>
<td>?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>IP Blocking</td>
<td>?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>BGP</td>
<td>?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>N/A</td>
</tr>
<tr>
<td>DNS</td>
<td>?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>N/A</td>
</tr>
<tr>
<td>Web Proxy</td>
<td>?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Real Time Monitoring</td>
<td>?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Deep Packet Inspection</td>
<td>?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Botnets

Storm

Chameleon

Mirai

Necurs
DDoS as a Service
DDoS as a Service

CRAZY FEATURES

Our high performance dedicated servers ensures only strong stress tests. With spoofed and amplified stress tests we take care of your privacy online.

Our custom coded attack scripts, IP Logger, 24/7 customer service, 37 backend servers, Layer4 and Layer7 stress tests, Paypal and Bitcoin autobuy.

Purchase using Paypal
We believe in huge potential of Paypal with paying online. Many other booters / IP Stressers doesn't have paypal enabled because they are scamming their customers.

Purchase with Bitcoin
By purchasing with bitcoin you automatically grant yourself a 15% discount. This beautiful crypto currency ensures complete privacy while paying online.
Remote Requests

- **Port Open**
  - Initial seq # for server to client bytes
  - Ack of client -> server ISN + 1

- **Port Closed**
  - No machine
  - ICMP response from router
  - Machine but port closed
  - TCP reset packet
  - Intercepted
  - Silence (depends on config)
Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-18 21:43 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td>OpenSSH 6.6.1 p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td>Apache httpd 2.4.7 ((Ubuntu))</td>
</tr>
<tr>
<td>554/tcp</td>
<td>open</td>
<td>rtsp</td>
<td></td>
</tr>
<tr>
<td>7070/tcp</td>
<td>open</td>
<td>realserver</td>
<td></td>
</tr>
<tr>
<td>9929/tcp</td>
<td>open</td>
<td>nping-echo Nping echo</td>
<td></td>
</tr>
<tr>
<td>31337/tcp</td>
<td>open</td>
<td>open</td>
<td>Elite</td>
</tr>
</tbody>
</table>

Device type: general purpose
Running (JUST GUESSING): Linux 3.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:3.13
Aggressive OS guesses: Linux 3.13 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 20.31 seconds
## Packet Filtering

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Dest. Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>*</td>
<td>192.168.1.*</td>
<td>25</td>
<td>Permit</td>
</tr>
<tr>
<td>UDP</td>
<td>*</td>
<td>192.168.1.*</td>
<td>69</td>
<td>Permit</td>
</tr>
<tr>
<td>TCP</td>
<td>192.168.1.*</td>
<td>*</td>
<td>80</td>
<td>Permit</td>
</tr>
<tr>
<td>TCP</td>
<td>*</td>
<td>192.168.1.18</td>
<td>80</td>
<td>Permit</td>
</tr>
<tr>
<td>TCP</td>
<td>*</td>
<td>192.168.1.*</td>
<td>*</td>
<td>Deny</td>
</tr>
<tr>
<td>TCP</td>
<td>*</td>
<td>192.168.1.*</td>
<td>*</td>
<td>Deny</td>
</tr>
</tbody>
</table>
Stateful Inspection
alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"OS-LINUX
OS-LINUX x86 Linux overflow attempt";
flow:to_server,established; content:"1|C0 B0 02 CD 80 85
C0|uL|EB|L^|B0|"; metadata:ruleset community, service dns;
class:attempted-admin; sid:264; rev:13;)

Deep-Packet Inspection
Network Security

Diagram:

- **Best-Case**:
  - You’re constantly being rescued from peril by a faceless team of engineers who could wander away at any time.

- **Worst-Case**:
  - Your appliance is part of a botnet run by organized crime.

- **How long you’ve had your smart appliance**:
  - 6 months
  - 1 year
  - 5 years
  - 10 years