Cyber Demo

Carolyn Lauzon – Department of Energy, Office of Science
Ti Leggett – Argonne Leadership Computing Facility
What is hacking and why?
Largest-Ever DDoS Campaign Demonstrates Danger of New Attack Method

By: Robert Lemos, eWeek

Largest-Ever DDoS Campaign Demonstrates Danger of New Attack Method
By: Robert Lemos, eWeek

DDOS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world
By: Damien Fletcher, Mirror
DDOS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world
By: Damien Fletcher, Mirror

Largest Ever DDoS Campaign Demonstrates Danger of New Attack Method
By: Robert Lemos, eWeek

Lloyds Bank services hit by denial-of-service attack
By: Danny Palmer, ZDNet
Largest-Ever DDoS Campaign Demonstrates Danger of New Attack Method
By: Robert Lemos, eWeek

DDoS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world
By: Damien Fletcher, Mirror

Mirai variant botnet launches IoT DDoS attacks on financial sector
By: Alison DeNisco Rayome, TechRepublic

Lloyds Bank services hit by denial-of-service attack
By: Danny Palmer, ZDNet
DDOS attack on Spamhaus: Largest Ever DDoS Campaign Demonstrates Danger of New Attack Method
By: Robert Lemos, eWeek

DDOS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world
By: Damien Fletcher, Mirror

Lloyds Bank services hit by denial-of-service attack
By: Danny Palmer, ZDNet

Mirai variant botnet launches IoT DDoS attacks on financial sector
By: Alison DeNisco Rayome, TechRepublic

Large DDoS attacks cause outages at Twitter, Spotify, and other sites
By: Darrell Etherington, TechCrunch
https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/
Largest Ever DDoS Campaign Demonstrates Danger of New Attack Method
By: Robert Lemos, eWeek

DDoS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world
By: Damien Fletcher, Mirror

Mirai variant botnet launches IoT DDoS attacks on financial sector
By: Alison DeNisco Rayome, TechRepublic

Lloyds Bank services hit by denial-of-service attack
By: Danny Palmer, ZDNet

Evidence suggests Stuxnet worm set Iran’s nuclear program back
By: Dean Takahashi, VentureBeat
https://venturebeat.com/2011/01/15/evidence-builds-that-stuxnet-worm-was-aimed-at-averting-war-over-irans-nuclear-weapons/

Large DDoS attacks cause outages at Twitter, Spotify, and other sites
By: Darrell Etherington, TechCrunch
https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/
The Internet and Cyber Security
A Simple Network of Computers Talking
Mini Demo: TinyTitan = Shows Computers Talking to Each Other Over a Network
Tiny Titan: A Simple Network of Computers Talking
Tiny Titan: A Simple Network of Computers Talking
Security Sam
Monitors Pis Traffic
Mini Demo:
Security Sam Traffic Monitoring on Pi1
Hacker Hal
Wants to Stop Pis from Sharing Secrets
What things might Hal do to stop Pis from sharing secrets?
What things might Hal do to stop Pis from sharing secrets?
What things might Hal do to stop Pis from sharing secrets?
What things might Hal do to stop Pis from sharing secrets?
What things might Hal do to stop Pis from sharing secrets?
What things might Hal do to stop Pis from sharing secrets?
What things might Hal do to stop Pis from sharing secrets?
Mini Demo:
Hacker Hal Strikes - Denial of Service (DoS)
Hacker Hal Strikes - Denial of Service (DoS)
Hacker Hal Not Effective

• What could Hal do to have an impact?
Hacker Hal Super Strike
Distributed Denial of Service (DDoS)
Hacker Hal Strikes Again - Distributed Denial of Service
Mini Demo: TinyTitan DDOS Impact
7 Iranians Indicted for DDoS Attacks Against U.S. Banks

By: Eric Chabrow, Bank Info Security

https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989
Overwhelm an Amazon distribution center

DDOS

• Amazon verifies:
  • Every delivery (3-way handshake)
    • Checks every truck and driver
  • Each package (integrity)
    • Scans package barcode

• You could send:
  • A few big trucks with lots of packages each, OR
    • Amazon is designed to handle this
  • Lots of cars with one package each
    • “Valid” deliveries, but not how Amazon was designed
Extra
ARP
Mac Address and IP Address
<table>
<thead>
<tr>
<th>Name</th>
<th>Mac Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>pi1</td>
<td>b8 : 27 : eb : 9f : 4e : c5</td>
<td>192.168.3.101</td>
</tr>
<tr>
<td>pi2</td>
<td>b8 : 27 : eb : be : 80 : c1</td>
<td>192.168.3.102</td>
</tr>
<tr>
<td>pi3</td>
<td>b8 : 27 : eb : 89 : 58 : fd</td>
<td>192.168.3.103</td>
</tr>
<tr>
<td>pi4</td>
<td>b8 : 27 : eb : 53 : 6a : eb</td>
<td>192.168.3.104</td>
</tr>
<tr>
<td>pi5</td>
<td>b8 : 27 : eb : dc : c0 : 0c</td>
<td>192.168.3.105</td>
</tr>
<tr>
<td>pi6</td>
<td>b8 : 27 : eb : c5 : 4f : 8f</td>
<td>192.168.3.106</td>
</tr>
<tr>
<td>pi7</td>
<td>b8 : 27 : eb : f2 : 3c : a9</td>
<td>192.168.3.107</td>
</tr>
<tr>
<td>pi8</td>
<td>b8 : 27 : eb : 7f : 25 : 09</td>
<td>192.168.3.108</td>
</tr>
<tr>
<td>pi9</td>
<td>b8 : 27 : eb : 79 : a1 : f8</td>
<td>192.168.3.109</td>
</tr>
</tbody>
</table>
Pi1 sends ‘secret’ to Pi2

A packet

Piece of Secret  Header
Pi1 sends ‘secret’ to Pi2

A packet

<p>| Piece of Secret | MAC address | IP address | + |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Mac Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>pi1</td>
<td>b8 : 27 : eb : 9f : 4e : c5</td>
<td>192.168.3.101</td>
</tr>
<tr>
<td>pi2</td>
<td>b8 : 27 : eb : be : 80 : c1</td>
<td>192.168.3.102</td>
</tr>
<tr>
<td>pi3</td>
<td>b8 : 27 : eb : 89 : 58 : fd</td>
<td>192.168.3.103</td>
</tr>
<tr>
<td>pi4</td>
<td>b8 : 27 : eb : 53 : 6a : eb</td>
<td>192.168.3.104</td>
</tr>
<tr>
<td>pi5</td>
<td>b8 : 27 : eb : dc : c0 : 0c</td>
<td>192.168.3.105</td>
</tr>
<tr>
<td>pi6</td>
<td>b8 : 27 : eb : c5 : 4f : 8f</td>
<td>192.168.3.106</td>
</tr>
<tr>
<td>pi7</td>
<td>b8 : 27 : eb : f2 : 3c : a9</td>
<td>192.168.3.107</td>
</tr>
<tr>
<td>pi8</td>
<td>b8 : 27 : eb : 7f : 25 : 09</td>
<td>192.168.3.108</td>
</tr>
<tr>
<td>pi9</td>
<td>b8 : 27 : eb : 79 : a1 : f8</td>
<td>192.168.3.109</td>
</tr>
</tbody>
</table>
Pi1 sends ‘secret’ to Pi2

A packet

Piece of Secret

b8 : 27 : eb : be : 80 : c1
192.168.3.102
+
Pi1’s ARP table

<table>
<thead>
<tr>
<th>Mac Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>b8 : 27 : eb : be : 80 : c1</td>
<td>192.168.3.102</td>
</tr>
<tr>
<td>b8 : 27 : eb : 89 : 58 : fd</td>
<td>192.168.3.103</td>
</tr>
<tr>
<td>b8 : 27 : eb : 53 : 6a : eb</td>
<td>192.168.3.104</td>
</tr>
<tr>
<td>b8 : 27 : eb : dc : c0 : 0c</td>
<td>192.168.3.105</td>
</tr>
<tr>
<td>b8 : 27 : eb : c5 : 4f : 8f</td>
<td>192.168.3.106</td>
</tr>
<tr>
<td>b8 : 27 : eb : f2 : 3c : a9</td>
<td>192.168.3.107</td>
</tr>
<tr>
<td>b8 : 27 : eb : 7f : 25 : 09</td>
<td>192.168.3.108</td>
</tr>
<tr>
<td>b8 : 27 : eb : 79 : a1 : f8</td>
<td>192.168.3.109</td>
</tr>
</tbody>
</table>
Evil Eve Evesdropper wants to spy on Pi1 and Pi2 secrets

MAC| b8 : 27 : eb : 00 : 96 : 8c
Evil Eve Evesdropper wants to spy on Pi1 and Pi2 secrets.
Evil Eve Evesdropper wants to spy on Pi1 and Pi2 secrets

Pi1,
192.168.3.102
is at
b8:27:eb:00:96:8c

MAC| b8 : 27 : eb : 00 : 96 : 8c
IP| 192.168.3.120
## P1’s ARP Table

<table>
<thead>
<tr>
<th>Mac Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>b8 : 27 : eb : be : 80 : c1</td>
<td>192.168.3.102</td>
</tr>
<tr>
<td>b8 : 27 : eb : 89 : 58 : fd</td>
<td>192.168.3.103</td>
</tr>
<tr>
<td>b8 : 27 : eb : 53 : 6a : eb</td>
<td>192.168.3.104</td>
</tr>
<tr>
<td>b8 : 27 : eb : dc : c0 : 0c</td>
<td>192.168.3.105</td>
</tr>
<tr>
<td>b8 : 27 : eb : c5 : 4f : 8f</td>
<td>192.168.3.106</td>
</tr>
<tr>
<td>b8 : 27 : eb : f2 : 3c : a9</td>
<td>192.168.3.107</td>
</tr>
<tr>
<td>b8 : 27 : eb : 7f : 25 : 09</td>
<td>192.168.3.108</td>
</tr>
<tr>
<td>b8 : 27 : eb : 79 : a1 : f8</td>
<td>192.168.3.109</td>
</tr>
</tbody>
</table>

192.168.3.120
b8 : 27 : eb : 00 : 96 : 8c
### P1’s ARP Table

<table>
<thead>
<tr>
<th>Mac Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>b8 : 27 : eb : 00 : 96 : 8c</td>
<td>192.168.3.102</td>
</tr>
<tr>
<td>b8 : 27 : eb : 89 : 58 : fd</td>
<td>192.168.3.103</td>
</tr>
<tr>
<td>b8 : 27 : eb : 53 : 6a : eb</td>
<td>192.168.3.104</td>
</tr>
<tr>
<td>b8 : 27 : eb : dc : c0 : 0c</td>
<td>192.168.3.105</td>
</tr>
<tr>
<td>b8 : 27 : eb : c5 : 4f : 8f</td>
<td>192.168.3.106</td>
</tr>
<tr>
<td>b8 : 27 : eb : f2 : 3c : a9</td>
<td>192.168.3.107</td>
</tr>
<tr>
<td>b8 : 27 : eb : 7f : 25 : 09</td>
<td>192.168.3.108</td>
</tr>
<tr>
<td>b8 : 27 : eb : 79 : a1 : f8</td>
<td>192.168.3.109</td>
</tr>
</tbody>
</table>

192.168.3.120
b8 : 27 : eb : 00 : 96 : 8c
Evil Eve Evesdropper spies on Pi1 and Pi2 Secrets
Evil Eve Evesdropper spies on Pi1 and Pi2 Secrets

Fix the header with correct MAC address
Evil Eve Evesdropper spies on Pi1 and Pi2 Secrets

Fix the header with correct MAC address
Screen Shots from “Evil Eve
Evil Eve ARP Table

root@kali:~# arp -a
?
(192.168.3.106) at b8:27:eb:c5:4f:8f [ether] on eth0
?
(192.168.3.104) at b8:27:eb:53:6a:eb [ether] on eth0
?
(192.168.3.103) at b8:27:eb:89:58:fd [ether] on eth0
?
(192.168.3.101) at b8:27:eb:9f:4e:c5 [ether] on eth0
?
(192.168.3.1) at <incomplete> on eth0
?
(192.168.3.109) at b8:27:eb:7d:a1:f8 [ether] on eth0
?
(192.168.3.107) at b8:27:eb:f2:3c:a9 [ether] on eth0
?
(192.168.3.105) at b8:27:eb:dc:c0:0c [ether] on eth0
?
(192.168.3.102) at b8:27:eb:be:80:c1 [ether] on eth0
?
(192.168.3.110) at b8:27:eb:2c:0d:f3 [ether] on eth0
?
(192.168.3.108) at b8:27:eb:7f:25:09 [ether] on eth0
root@kali:~#
Evil Eve ARP Spoof

<table>
<thead>
<tr>
<th>Evil Eve Mac</th>
<th>pi1 mac</th>
<th>arp reply</th>
<th>pi2 IP</th>
<th>is – at</th>
<th>Evil Eve Mac</th>
</tr>
</thead>
</table>
Evil Eve ARP Spoof and Unspoof

Cleaning up and re-arping targets...
DEMO
EXTRA EXTRA
Tiny Titan: A Simple Network of Computers Talking
“Need to add ‘Security Sam’. Security Sam is a Pi and has tap into all traffic INTO Pi1.”
Hacker Hal
Wants to Steal Secrets from Pi1 and Pi2
Hacker Hal
Tricks Pi1 into thinking HH is Pi2
Hacker Hal
Tricks Pi2 into thinking HH is Pi1

“Im Pi1”
Mini Demo:
Stealing Secrets: “ARP” Poisoning
Acknowledgement

Adam Simpson (Oak Ridge National Laboratory, NVIDIA) and Robert French (Oak Ridge National Laboratory) for support with Tiny Titan.

This presentation used resources of the Argonne Leadership Computing Facility at Argonne National Laboratory, which is supported by the Office of Science of the U.S. Department of Energy, Office of Science, under contract number DE-AC02-06CH11357.