IDS, NAT, and Online Privacy Management

DR KAMI VANIEA
First the news...
Tutorials/Labs

• New times!
  ◦ Monday 12-1pm,
  ◦ Tuesday: 9am-10am
  ◦ Wed: 11am-12pm
  ◦ Fri: 10am-11am

• All in Forest Hill 3.D01
Today

• Intrusion Detection Systems (IDS)
• Network Address Translation (NAT)
• Data leakage on the web
  ◦ Why it matters
  ◦ What it looks like
  ◦ How to protect yourself
Intrusion Detection Systems (IDS)
Firewalls are preventative, IDS detects a potential incident in progress

• At some point you have to let some traffic into and out of your network (otherwise users get upset)

• Most security incidents are caused by a user letting something into the network that is malicious, or by being an insider threat themselves

• These cannot be prevented or anticipated in advance

• The next step is to identify that something bad is happening quickly so you can address it
Signature based

- Perform simple pattern matching and report situations that match the pattern
- Requires that admin anticipate attack patterns in advance
- Attacker may test attack on common signatures
- Impossible to detect a new type of attack
- High accuracy, low false positives
Heuristic based

• Dynamically build a model of acceptable or “normal” behavior and flag anything that does not match
• Admin does not need to anticipate potential attacks
• System needs time to warm up to new behavior
• Can detect new types of attacks
• Higher false positives, lower accuracy
Number of alarms is a big problem

- In the Target breach the IDS did correctly identify that there was an attack on the Target network
- There were too many alarms going off to investigate all of them in great depth
- Some cyberattack insurance policies state that if you know about an attack and do nothing they will not cover the attack.
- Having a noisy IDS can potentially be a liability
Network Address Translation (NAT)
Looking at the IP address of my laptop which is connected to the University WIFI.
My computer as seen from a remote server
(http://www.hashemian.com/whoami/)

My IP previously showed as: 172.20.106.96

What happened?

REMOTE_ADDR: 192.41.131.255
REMOTE_PORT: 7535
REQUEST_METHOD: GET
REQUEST_TIME: 1474906336
REQUEST_URI: /whoami/
SERVER_ADDR: 173.162.146.61
SERVER_NAME: www.hashemian.com
SERVER_PORT: 80
SERVER_PROTOCOL: HTTP/1.1
SERVER_SIGNATURE:
SERVER_SOFTWARE: Apache
IPv4 and address space exhaustion

• Version 4 of the Internet Protocol
  ◦ 192.168.2.6
• There are less than 4.3 billion IPv4 addresses available
• We do not have enough addresses for every device on the planet
• Answer: Network Address Translation
  ◦ Internal IP different than external IP
  ◦ Border router maps between its own IP and the internal ones
Each number is an AS, which is a network run by a single group.

Each colored line is the current shortest path between two AS’s. All lines on this graph connect Syria to other parts of the world.

Syria’s AS is, directly connected to three other AS’s.

Paths shift all the time. This is normal on the internet as the current shortest path is dynamically negotiated (BGP routing).
Each number is an Autonomous System (AS)

Each AS has the ability to manage its own IPs how it sees fit

Each network has a similar ability
Internet
Home
Router
Wireless Access Point
Mobile Devices
Desktop PCs and laptops
Boundary Firewall
Email, web and application servers
Databases
Card Readers
3rd party server

192.168.4.2
192.168.4.0
173.162.146.61
10.24.54.65
192.41.131.255
192.168.4.1
192.168.4.2
192.168.4.0
My laptop can have multiple IPs and bridge networks too. Here it shows IPs for both my VirtualBox and my WIF.
Online Privacy Management
The following is copied from talks I give groups like lawyers, policy makers, and the general public about privacy protections.

I have added some extra technical details, but these are the kinds of issues they worry about.
Firefox add-ons

- The following set of screenshots were created using these addons. These are all safe to download and use from home.
  - Tilt
  - uMatrix
  - Ghostery
  - Lightbeam
  - Firebug
  - Built-in Firefox developer tools
Web pages are built dynamically
Websites are made up of many elements from many sources
Let's take a look at how The Guardian's website is built dynamically.
The Guardian: content sources

- guim.co.uk
- ophan.co.uk
- revsci.net
- guardianapps.co.uk
- scorecardresearch.com
- googleadservices.com
- doubleclick.net
- imrworldwide.com
- krxd.net
- google.com
- google.co.uk
- d935jy3y59lth.cloudfront.net
- rubiconproject.com
- dqwufkbc3sdtr.cloudfront.net
- d1mbyzj6lih1pj.cloudfront.net
- googlesyndication.com
- googletagservices.com
- adnxs.com
- moatads.com
The Telegraph: content sources

- optimizely.com
- d3c3cq33003psk.cloudfront.net
- quantserve.com
- ooyala.com
- google.com
- criteo.com
- parsely.com
- visualrevenue.com
- googletagservices.com
- effectivemeasure.net
- demdex.net
- outbrain.com
- youtube.com
- ytimg.com
- omtrdc.net
- akamaihd.net
- scorecardresearch.com
- doubleclick.net
- disqus.com
- skimresources.com
- qubitproducts.com
- serving-sys.com
- googlesyndication.com
- moatads.com
- adsafeprotected.com
- imrworldwide.com
- opta.net
- twitter.com
- vdna-assets.com
- mediavoice.com
- krxd.net
- msn.com
- bing.com
- t.co
- visualdna.com
- facebook.net
- polarmobile.com
- matheranalytics.com
- facebook.com
- chartbeat.com
- chartbeat.net
- d3ujids68p6xmq.cloudfront.net
- pagefair.com
- pagefair.net
- ml314.com
- linkedin.com
- chartbeat.net
- clarifyingquack.com
- flappysquid.net
- mathtags.com
- rlcdn.com
The Guardian: content sources

- guim.co.uk
- ophan.co.uk
- revsci.net
- guardianapps.co.uk
- scorecardresearch.com
- googleadservices.com
- doubleclick.net
- imrworldwide.com
- krxd.net
- google.com
- google.co.uk
- d935jy3y59lth.cloudfront.net
- rubiconproject.com
- dqwufkbc3sdtr.cloudfront.net
- d1mbyzj6lih1pj.cloudfront.net
- googlesyndication.com
- googletagservices.com
- adnxs.com
- moatads.com
The Guardian: content sources

**Content Delivery**
- guim.co.uk
- guardianapps.co.uk
- d935jy3y59lth.cloudfront.net
- dqwufkbc3sdtr.cloudfront.net
- d1mbyzj6lih1pj.cloudfront.net

**Trackers / Other**
- scorecardresearch.com
- rubiconproject.com
- adnxs.com
- moatads.com
- revsci.net
- imrworldwide.com
- krxd.net
- doubleclick.net
- google.com
- google.co.uk
- googleleadservices.com
- googletagservices.com
- google syndication.com
- ophan.co.uk
Javascript
✓ theguardian.com
✓ Guardian owned
✘ Others

Content
✓ theguardian.com
✓ Guardian owned
✘ Others
Javascript
✓ theguardian.com
✓ Guardian owned
✓ Others

Content
✓ theguardian.com
✓ Guardian owned
✓ Others
Reloaded

Javascript
✓ theguardian.com
✓ Guardian owned
✓ Others

Content
✓ theguardian.com
✓ Guardian owned
✓ Others
Who cares?
What is the best predictor for being compromised?
Malicious payloads were being delivered to around 300,000 users per hour. The company guesses that around 9 percent of those, or 27,000 users per hour, were being infected.
“Clients visiting yahoo.com received advertisements served by ads.yahoo.com. Some of the advertisements are malicious ... Instead of serving ordinary ads, the Yahoo's servers reportedly sends users an ‘exploit kit.’”
“Ya, but website owners are careful about the content they present to users... I can trust big websites.”
Loading all content

Only loading content from theguardian.com
<html>
<body>
  Hello World!
  <img src="http://example.com/img5.jpg"/>
  <script src="http://example.com/script.js"/>
</body>
</html>
Exclusive
Brexiters stoking intolerance with immigration obsession, says Cameron

PM criticises narrow focus of Farage, Gove and Hilton and says remain vote would show rejection of insular view

Live / Poll gives one-point lead to remain

Boris Johnson / I'll make TV apology if there's a recession

Mail Online / We don't stoke fears about immigration, says publisher
<html>
<body>
  Hello World!
  <img src="http://example.com/img5.jpg"/>
  <script src="http://example.com/script.js"/>
</body>
</html>
Listed in the URL bar - sometimes used to connect data between sites. The Unique ID indicating the exact image requested and other information about the user is included in the request headers.
Hello World!

<img src="http://example.com/img5.jpg"/>

<script src="http://example.com/script.js"/>
<html>
<body>
  Hello World!
  <img src="http://example.com/img5.jpg"/>
  <script src="http://adsense.com/script.js"></script>
</body>
</html>
Questions