IDS, NAT, and Online Privacy Management

Tutorials/Labs

- New times!
  - Monday 12-1pm,
  - Tuesday: 9am-10am
  - Wed: 11am-12pm
  - Fri: 10am-11am
- All in Forest Hill 3.001

First the news...

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)
My computer as seen from a remote server

My IP previously showed as: 172.20.106.96

What happened?

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 Autonomous System (AS)
Each AS has the ability to manage its own IP how it sees fit
Each network has a similar ability

Sample Network

Paths shift all the time. This is normal on the internet as the current shortest path is dynamically negotiated (BGP routing).
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

Let's take a look at how The Guardian's website is built dynamically

Zoomed out...

Loading all content

Only loading content from theguardian.com

The Guardian: content sources

- guim.co.uk
- orphan.co.uk
- revesci.net
- guardianapps.co.uk
- scorecardresearch.com
- googleadservices.com
- doubleclick.net
- imrworldwide.com
- krav.net

- google.com
- google.co.uk
- d1935yqy39h.cloudfront.net
- rubiconproject.com
- dwqbfk3sdr.cloudfront.net
- d1nbyz76ilh1pj.cloudfront.net
- googleadservices.com
- googletag.services.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
- t.co
- visualdna.com
- facebook.net
- polarmobile.com
- matheranalytics.com
- facebook.com
- chartbeat.com
- d3ujids68p6xmq.cloudfront.net
- pagefair.com
- pagefair.net
- ml314.com
- linkedin.com
- chartbeat.net
- clarifyingquack.com
- flappysquid.net
- mathtag.com
- rlcdn.com
- scorecardresearch.com
- doubleclick.net
- imworldwide.com
- krd.net
- adsafeprotected.com
- imrworldwide.com
- opta.net
- twitter.com
- vdna.assets.com
- mediavoice.com
- krxd.net
- msn.com
- bing.com

The Guardian: content sources
- guim.co.uk
- ophan.co.uk
- revsci.net
- guardianapps.co.uk
- scorecardresearch.com
- googleadservices.com
- doubleclick.net
- imworldwide.com
- krd.net
- google.com
- google.co.uk
- d935jy3y59lth.cloudfront.net
- rubiconproject.com
- dwufkbc3dstr.cloudfront.net
- d1mbyzj6ihl.p.cloudfront.net
- googleadservices.com
- googletagservices.com
- adnex.com
- moatads.com

Content Delivery
- guim.co.uk
- guardianapps.co.uk
- d935jy3y59lth.cloudfront.net
- dwufkbc3dstr.cloudfront.net
- d1mbyzj6ihl.p.cloudfront.net

Trackers / Other
- scorecardresearch.com
- rubiconproject.com
- adnex.com
- moatads.com
- imrworldwide.com
- krd.net
- doubleclick.net
- google.com
- google.co.uk
- googleadservices.com
- googletagservices.com
- adnex.com
- moatads.com

Javascript
- theguardian.com
- Guardian owned
- Others

Content
- theguardian.com
- Guardian owned
- Others
What is the best predictor for being compromised?

Who cares?
Thousands of visitors to yahoo.com hit with malware attack, researchers say

"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."
Hello World!

Questions