“The Trouble with Assumptions

Inveniamviamautfaciam

“What Assumption?”

- The dictionary definition of an 'assumption' is:
  “something taken for granted; a supposition

- The dictionary definition of an 'source ip' is:
  “(Internet Protocol address) The address of a device attached to an IP network (TCP/IP network). Every client, server and network device is assigned an IP address, and every IP packet traversing an IP network contains a source IP address and a destination IP address.”

- The assumption is that the source IP address is a valuable source of information

“What are we told?”

“Identifies traffic originating from bots and known malicious sources to stop automated attacks” - http://www.imperva.com/products/wsc_web-application-firewall.html

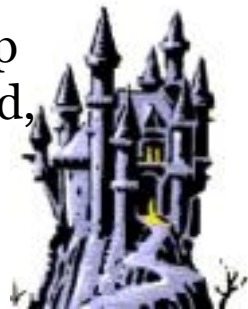
“There are numerous benefits for implementing blacklisting filters in the firewall” - https://dl.acm.org/citation.cfm?id=1566476

“An intruder blacklist is maintained by the daemon, using ipset. This blacklist is stored in memory by ipset.”- http://wiki.mandriva.com/en/Projects/Interactive_Firewall

“Mac OS X v10.6 uses an adaptive firewall that dynamically generates a firewall rule if a user has 10 consecutive failed login attempts. The generated rule blocks the user’s computer for 15 minutes, preventing the user from attempting to log in.” - http://blog.lastinfirstout.net/2011/04/os-x-adaptive-firewall-automated.html

“A netfilter firewall can blacklist hosts dynamically. This is very useful to stop hosts from performing brute force attacks on services that require a password, such as the ssh service.” - http://olivier.sessink.nl/publications/blacklisting/index.html

Invenia mviam autfacia m



“External Example”

• The advice on the previous page is well known, but are our assumptions about using the source IP address still so valid?

<run the external demo>

“More of what we are told”

For the correct routing, every intermediate router must have a routing table to know where to send the packet next. These routing tables are one of the best sources of information if investigating a digital crime and trying to track down an attacker. To do this, it is necessary to follow the packets of the attacker, reverse the sending route and find the computer the packet came from (i.e., the attacker).
https://en.wikipedia.org/wiki/Network_forensics

Here we are discussing a post investigation aspect of above and similar scenarios i.e. what after once the source IP Address (of the attacker) is identified? In this article we are going to discuss about a simple tool/script, which helps forensic analyst to get the exact location of the source IP Address on this very beautiful earth.
http://niiconsulting.com/checkmate/2010/01/06/geoedge-ip-address-locator/

Network forensics goes beyond simple network activity monitoring. An activity monitoring solution may flag a suspicious incident, but it requires sorting through possibly thousands of packets of data – which can include IP address, source/destination port, time, date, protocol, string and more – to find that one incident again
http://www.infosecurity-magazine.com/view/21070/comment-network-forensics-beyo

Invenia mviamautfaciam

“Internal Examples”

• You have the logs! You have the incident identified! You have the source ip! Now you can get the bag guy …. right ?

<internal demo 1>

• Ok, that’s bad, but the scope is limited … right?

<internal demo 2>

“The future of defence and attack?”

- The attackers will continue to come up with news ways to not get caught
- Tonight we only looking at one of our security assumptions
- Dealing with our assumptions is difficult
- The best defence is knowledge and an open mind

Invenia mviam autfaciam

Thank you for your attention

Questions?

Inveniam viam aut faciam