Planning

Wednesday, January 2, 2019 3:24 PM

Scope

Wednesday, January 2, 2019 3:30 PM

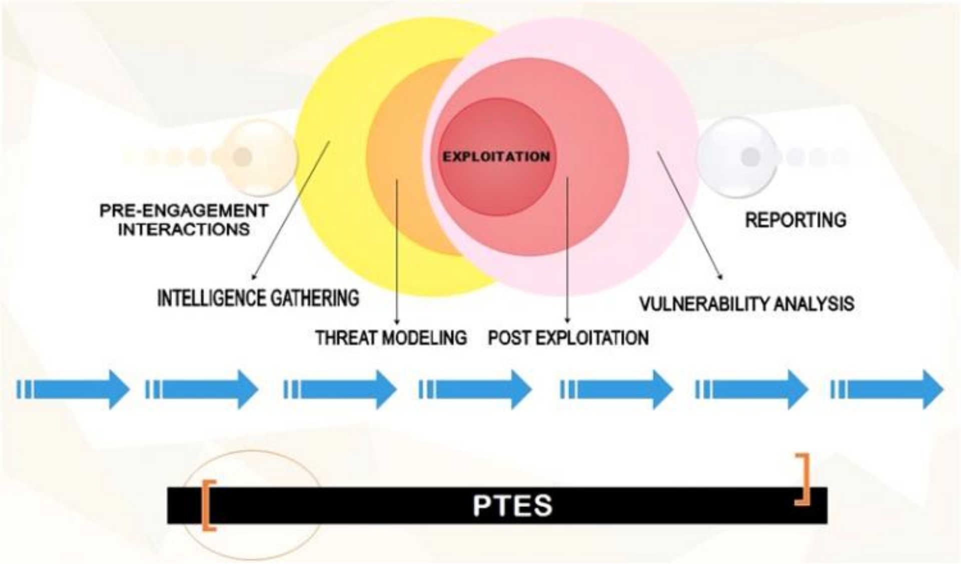
https://www.google.com/search?rlz=1C1GCEB_enUS786US786&ei=i08tXP3CLqu2gge_uLf4Bg&q=penetration+testing+scope&oq=penetration+testing+scope&gs_l=psy-ab.3..0j0i20i263j0l8.49317.50917..51094...0.0..1.847.3438.3-2j0j2j2......0....1..gws-wiz.......0i71j35i39j0i67.5lF6HHw-amk

Intel Gathering

Sunday, December 23, 2018 1:41 AM

Introduction: Intelligence Gathering & Its Relationship to the Penetration Testing Process
Penetration testing simulates real cyber-attacks, either directly or indirectly, to circumvent security systems and gain access to a company's information assets. The whole process, however, is more than just playing automated tools and then proceed to write down a report, submit it and collect the check.

The Penetration Testing Execution Standard (PTES) is a norm adopted by leading members of the security community as a way to establish a set of fundamental principles of conducting a penetration test. Seven phases lay the foundations of this standard: Pre-engagement Interactions, Information Gathering, Threat Modeling, Exploitation, Post Exploitation, Vulnerability Analysis, Reporting.



Intelligence gathering is the first stage in which direct actions against the target are taken. One of the most important ability a pen tester should possess is to know how to learn as much as possible about a targeted organization without the test has even begun – for instance, how this organization operates and its day-to-day business dealings – but most of all, he should make any reasonable endeavor to learn more about its security posture and, self-explanatory, how this organization can be attacked effectively. So, every piece of information that a pen tester can gather will provide invaluable insights into essential characteristics of the security systems in place.

What is the Difference Between Active and Passive Information Gathering?
Information Gathering is at times referred to as Open Source Intelligence (OSINT). The OSINT may come in three different forms:

Active Information Gathering – under this method, the targeted organization may become aware of the ongoing reconnaissance process since the pentester is actively engaging with the target. During this phase, he takes an active part in mapping network infrastructure, then he enumerates and/or scans the open services for vulnerabilities, and eventually searches for unpublished directories, files and servers. Other similar activities include OS Fingerprinting, Banner grabbing, and Web server application scan.
Active information gathering requires more preparation from the person who performs it because it leaves traces, which are likely to alert the target or produce evidence against him in the course of a possible digital investigation. According to the predominant opinion of experts in the information security sector, however, the information gathering process is based to a great extent on the notion of passive reconnaissance whose goal is to collect information about the target via publicly available resources only. Therefore, the other two forms are considered typical of what is actually information gathering.

Semi-passive Information Gathering – in accordance with this technique, profiling of the target is done through methods that would successfully mimic regular Internet traffic and behavior. It would mean that conducting in-depth reverse lookups, brute force DNS requests is out of the question, or even searching for "unpublished" servers or directories. Nevertheless, variations of these techniques are permitted so long as they penetrate with a feather-light touch. Other telltale acts that a pentester should restrain himself from doing are running network level portscans or crawlers. What is allowed, then? In a nutshell, querying only published name servers for relevant information and looking at metadata in published documents and files. As with the Passive Information Gathering phase, it all comes down to not drawing attention to any pentest activities whatsoever. Presumably, post-mortem discoveries on the target's part are possible, but only up to a point that leads to a dead end.

Passive Information Gathering – this option is under discussion provided that there is an explicit demand for the gathering activities not to be detected by the target. In this regard, the pentester cannot use tools that send traffic to the targeted company neither from his host nor an "anonymous" one across the Internet. Not only will that be technically burdening but also the person who performs the pentest will have to substantiate his findings with whatever he can dig out from archived or stored information, which is at times not up to date and incorrect because it has been limited to inquiries collected from third parties.
Passive reconnaissance activities may include (but are not limited to): Identifying IP Addresses and Sub-domains, Identifying External/3rd Party sites, Identifying People, Identifying Technologies, Identifying Content of Interest, Identifying Vulnerabilities. Once again, none of these techniques involve intrusive scanning or probing a given website. Instead, all of this information is to be gathered from the public domain, using techniques and tools readily available to anyone. It all may start, in fact, with conducting manual research into the company's website for useful information as:

Company contact names, phone numbers and email addresses
Company locations and branches
Other companies with which the target company partners or deals
News, such as mergers or acquisitions
Links to other company-related sites
Company privacy policies, which may help identify the types of security mechanisms in place
Other resources that may provide information about the targeted organization:
The SEC's EDGAR database if the company is publicly traded

Job boards, either internal to the company or external sites
Disgruntled employee blogs and Web sites
Trade press

So, in summary, active reconnaissance relies on traffic being sent to the targeted machine whereas, on the other hand, a pentester performing passive reconnaissance should make do with whatever information he can accumulate from the Internet. The former type is de facto undetectable, and the later one is a head-on confrontation of sorts so that the target machine may notice it.

Remember that every element of the penetration testing process should be executed within the scope of the sanctioned pentest. In this connection, passive reconnaissance may be the only method allowed in some cases, since it is fairly unobtrusive.

The key point here is that exploitation is certainly important, but performing a thorough recon could prove very helpful at a later stage and also make the entire pentest go easier, faster and stealthier.

Social Engineering in the Context of Intelligence Gathering

Although social engineering is typically considered a form of passive or semi-passive information gathering, some forms of social engineering may fall into the "active reconnaissance" category.

Social engineering is deemed one of the most widespread avenues for gathering information on a particular individual or a firm. A lot of information is out there – just check the popular social media websites. Also, websites like Pipl, PeekYou, and Spokeo may come in handy as they will provide access to email addresses, locations, phone numbers, and even family tree information.

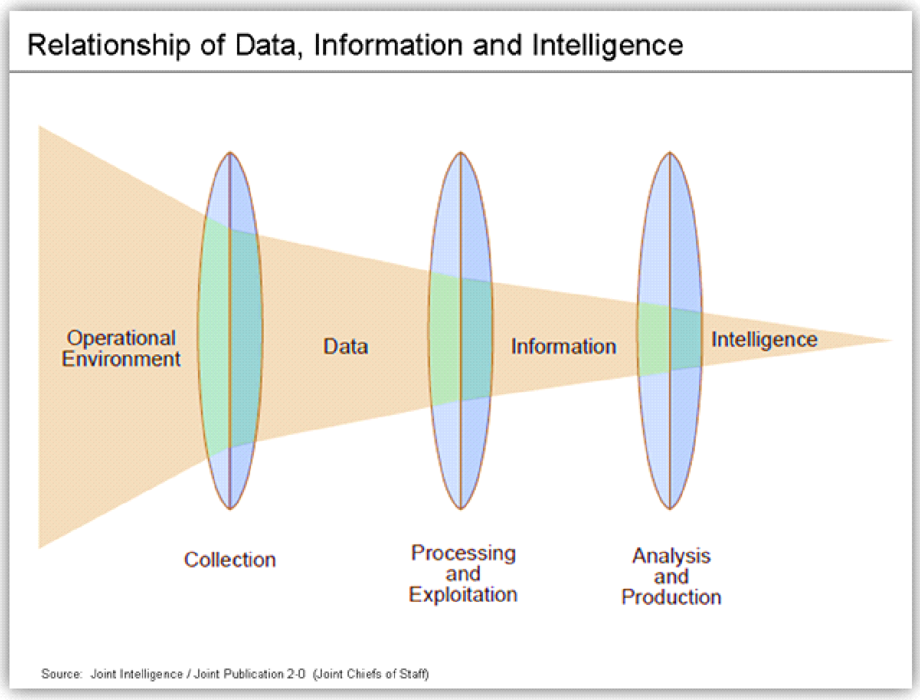
Clusters of seemingly unrelated information, such as products, services, business partners, suppliers, and analysis of information shared on corporate websites, for example, can proof valuable to understand the targeted organization better. Once you become acquainted with the "internal affairs" of the organization in question, you can try to come up with crafty social engineering schemes to help you replenish your reconnaissance well of information. A telephone call to the company's help desk may deliver to you any information, even privileged information if you are inventive enough (the so-called vishing). They offer a job, so why don't you give them a call or write an email to ask them questions, inter alia, about the organization?

While the term 'dumpster diving' means literally to rummage through someone else's trash, in the cybersecurity, it has a connotation of searching for all kinds of files which may divulge sensitive information like passwords and access codes written down on sticky notes 'in perfect Spanish scrawl.' Seemingly innocuous information, such as an organizational chart, calendar, and phone list, may assist a pentester in creating vicious social engineering scams to gain access to the targeted company's network.

Eavesdropping – finding key places to stay without attracting attention is important. Ideally, you can play with your phone in the middle of a room full of people that share inside information among themselves which you cannot help but overhear. Such hot-spots are a café, bar or restaurant across the street from your target site. Timing is the key – eavesdropping is being in the right place at the right time.

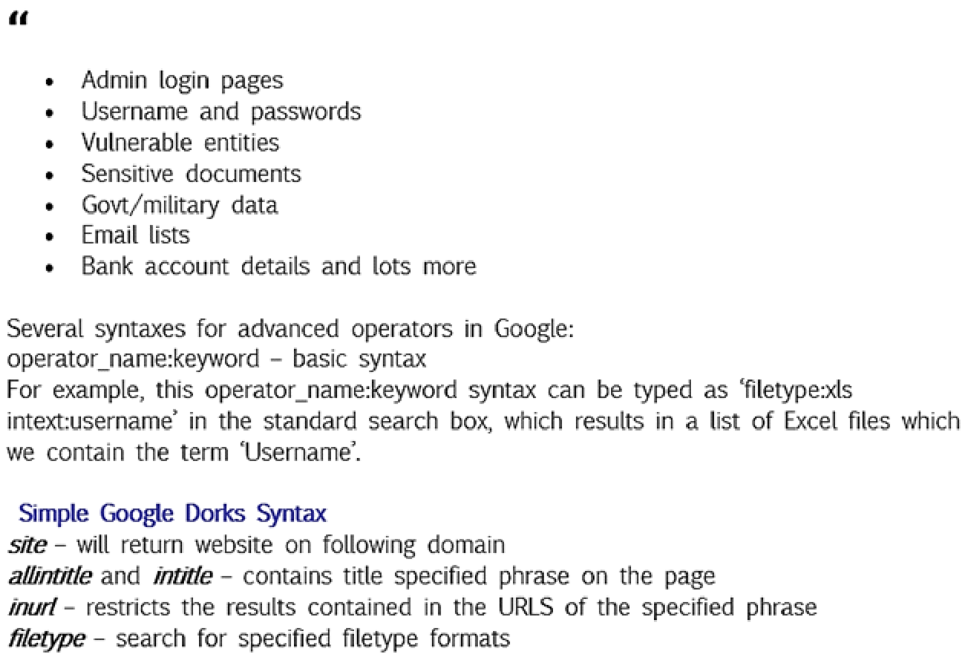
Shoulder Surfing – this is a variation of eavesdropping; instead of straining his years to hear something intriguing, the person who performs intelligence gathering attempts to obtain useful information, i.e., passwords, PINs, security codes, and similar data, by looking over someone's shoulder.

Establishing behavioral patterns (access paths, dress code, key locations, persons of interests, etc.) is part of the social engineering. With the help of services such as a touchgraph (i.e., a visual representation of social interactions between people) and Hoovers profile (which compiles various data on companies and produces a simplistic view on the business), you will perhaps be able to crunch big data and set the stage for a successful social engineering scenario. Maltego is another excellent tool that would allow you to assemble and arrange in a logical way research results leading to profiling of individuals.


Relationship of Data, Information and Intelligence
Operational Environment
Data
Information
Intelligence
Collection
Processing and Exploitation
Analysis and Production
Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

Google Hacking Overview

A pentester can use search tips called Google Hacks or Google Dorks to learn what Google knows about the targeted website. Google Hacking is a term used to describe a process of effective utilization of search operators that may reveal security vulnerabilities or misconfigurations in websites. A Google Dork query is a search string that makes use of advanced search operators to unearth information that is not immediately available. As a result, pentesters frequently benefit from Google Hacking to find vulnerabilities, secret sensitive information and access page in given websites indexed by Google's searching algorithm. Google Hacking can uncover the following information:



“

- Admin login pages
- Username and passwords
- Vulnerable entities
- Sensitive documents
- Govt/military data
- Email lists
- Bank account details and lots more

Several syntaxes for advanced operators in Google:
operator_name:keyword – basic syntax
For example, this operator_name:keyword syntax can be typed as ‘filetype:xls intext:username’ in the standard search box, which results in a list of Excel files which we contain the term ‘Username’.

Simple Google Dorks Syntax

site – will return website on following domain
allintitle and ***intitle*** – contains title specified phrase on the page
inurl – restricts the results contained in the URLS of the specified phrase
filetype – search for specified filetype formats

Source: Google Dorks: An Easy Way of Hacking by fr4nc1stein

Google Hacking Database created by Offensive Security is a very good source for passive Google-based vulnerability discovery. This website possesses a great number of Google hacks whose purpose is to mark specific vulnerabilities based on published advisories.

As a rule of thumb, a penetration test should begin with a passive reconnaissance phase. Public search engines have amassed enormous quantities of information on virtually every website on the Internet. Therefore, one should always give Google Hacking a go. It might surprise you when finding pieces of data so revealing you cannot help but wonder how this is supposed to be left in the open. By way of illustration, if the target has placed sensitive data in publicly available folders on his web server and in the web root (www or public_html), then Google and every other search engine can crawl it. On top of that, most of these directories are not password protected. All this information is publicly available, albeit the website’s owner consent.

Network mapping is an essential part of information gathering, and Google Hacking can also be used to locate the subdomain of the target website.

DNS Analysis

The Domain Name System translates easily to memorize, from a human point of view, domain names to numerical IP addresses necessary for locating and identifying computer devices and services with underlying network protocols. Misconfiguration in DNS nameservers, however, may lead to security vulnerabilities that will cause, among other things, information leakage concerning the domain. The DNS conversion forms itself in a local cache or a zone file on the server.

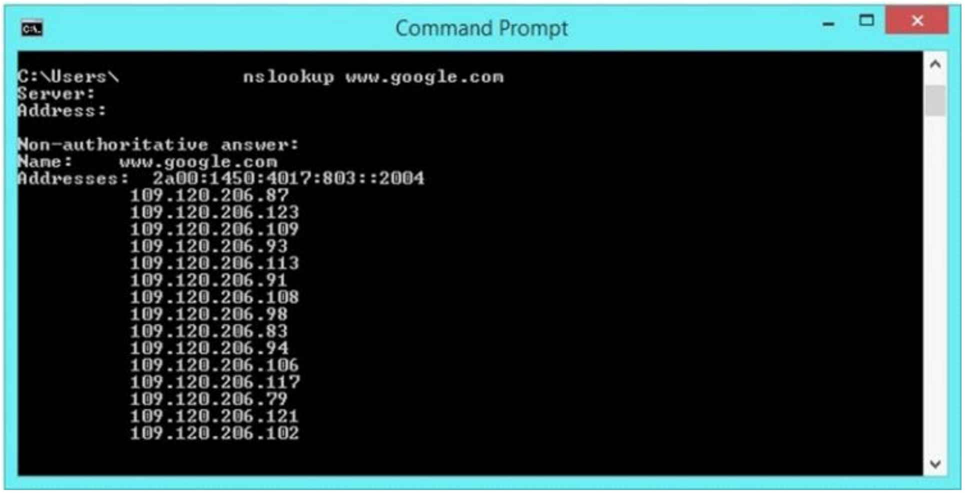
To put it in simple terms, a DNS lookup is when you use a domain name to find an IP address, and the Reverse DNS lookup works the other way around. The forward DNS lookup is the more common option. The whole process starts immediately after the user enters the web address (formally called URL) into his browser, which is first transmitted to the nearby router and then the forward DNS lookup is placed in a routing table to locate the IP address.

A set of information linked to it each domain the moment it is created: IP addresses, registration/creation date, owner of the domain, name servers, domain availability, etc. One can obtain this information and perform DNS lookup through multiple ways:

Online tools available for DNS lookup:

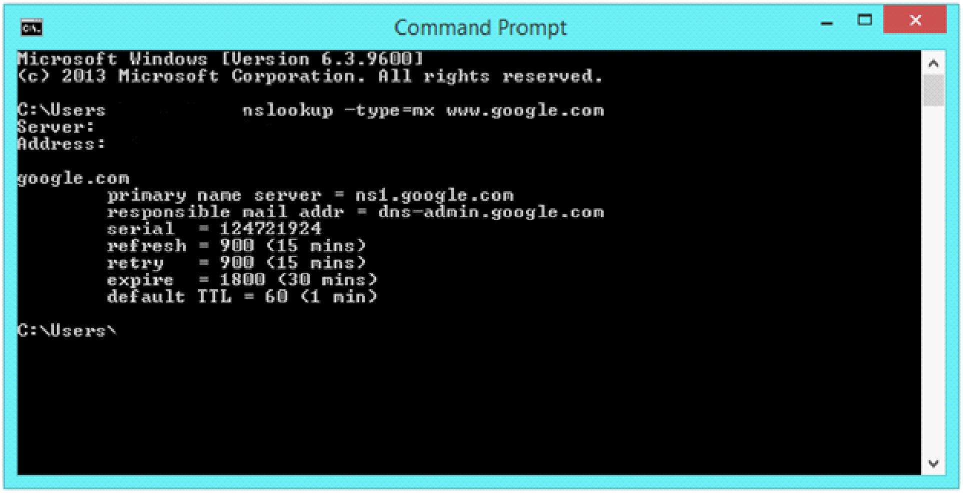
DNS Stuff
Domain Tools
Open Directory Web Tools
DNS Watch
Into DNS
Network Tools
Security Space WhoIs Gateway
MX Toolbox

Nslookup – it is a tool that one can run on Linux and Windows. It can be used to perform forward and reverse DNS lookups and query DNS server to derive intelligible information about the host machine. Open the command prompt in your Windows machine and type ‘nslookup’ + the domain name.



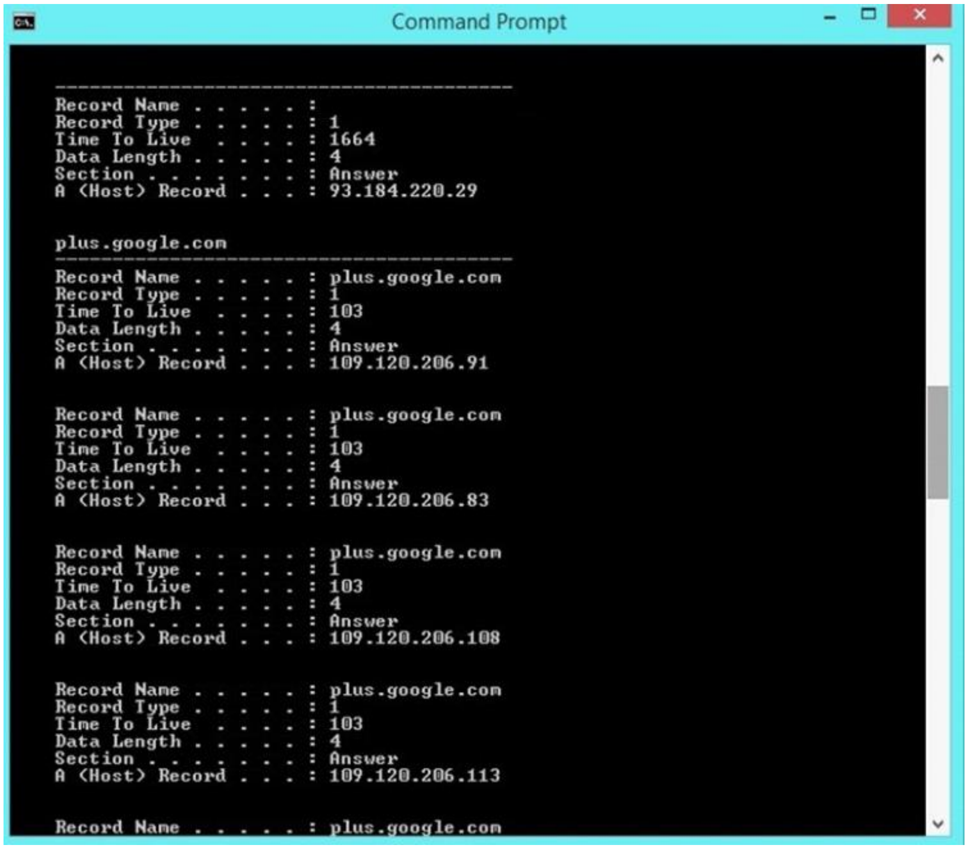
```
C:\Users\            nslookup www.google.com
Server:
Address:

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:4017:803::2004
          109.120.206.87
          109.120.206.123
          109.120.206.109
          109.120.206.93
          109.120.206.113
          109.120.206.91
          109.120.206.108
          109.120.206.98
          109.120.206.83
          109.120.206.94
          109.120.206.106
          109.120.206.117
          109.120.206.79
          109.120.206.121
          109.120.206.102
```

Adding ‘-type=mx’ parameter to the nslookup command will produce more information. Example: nslookup -type=mx www.google.com



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users              nslookup -type=mx www.google.com
Server:
Address:

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 124721924
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)

C:\Users\
```

IP Config Command – it will display DNS information – Record Name, Record Type, PTR Record, A-Host Record, Time to Live, Data Length, Section – regarding which websites a machine has visited from the moment cache was last created. Ipconfig /displaydns is the syntax for the ipconfig command.



```
    ----------------------------------------
    Record Name . . . . . :
    Record Type . . . . . : 1
    Time To Live  . . . . : 1664
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 93.184.220.29


    plus.google.com
    ----------------------------------------
    Record Name . . . . . : plus.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 103
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 109.120.206.91


    Record Name . . . . . : plus.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 103
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 109.120.206.83


    Record Name . . . . . : plus.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 103
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 109.120.206.108


    Record Name . . . . . : plus.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 103
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 109.120.206.113


    Record Name . . . . . : plus.google.com
```

Host Command – A Linux-driven DNS Lookup that reveals the IP address for a domain or host name. Syntax: host www.yoursite.com.

Dig is another handy Windows and Linux-based DNS lookup tool.

As aforementioned, the reverse DNS lookup reverses the process through entering the IP address to acquire the domain/host name.

> “
> Here is an example of using `nslookup` to do a reverse DNS lookup on the IP address 216.136.204.117:

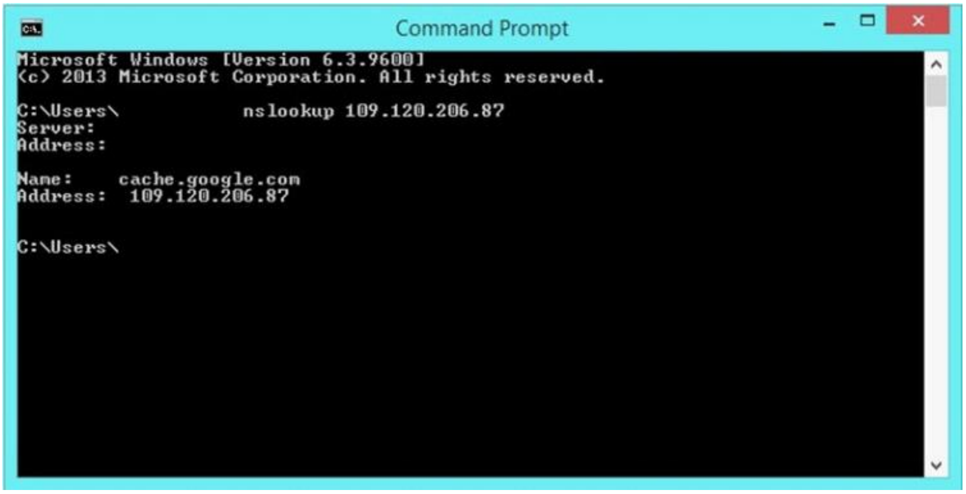
```
bash-2.05a$ nslookup 216.136.204.117
Server: localhost.net
Address: 127.0.0.1

Name: www.freebsd.org
Address: 216.136.204.117
```

> “
> The simplest way to perform a Reverse DNS Lookup is to use the *ping* command.

```
ping -a <xxx.xxx.xxx.xxx>
```

Similarly, you can also use the *nslookup* command with an IP address.

```
nslookup <xxx.xxx.xxx.xxx>
```



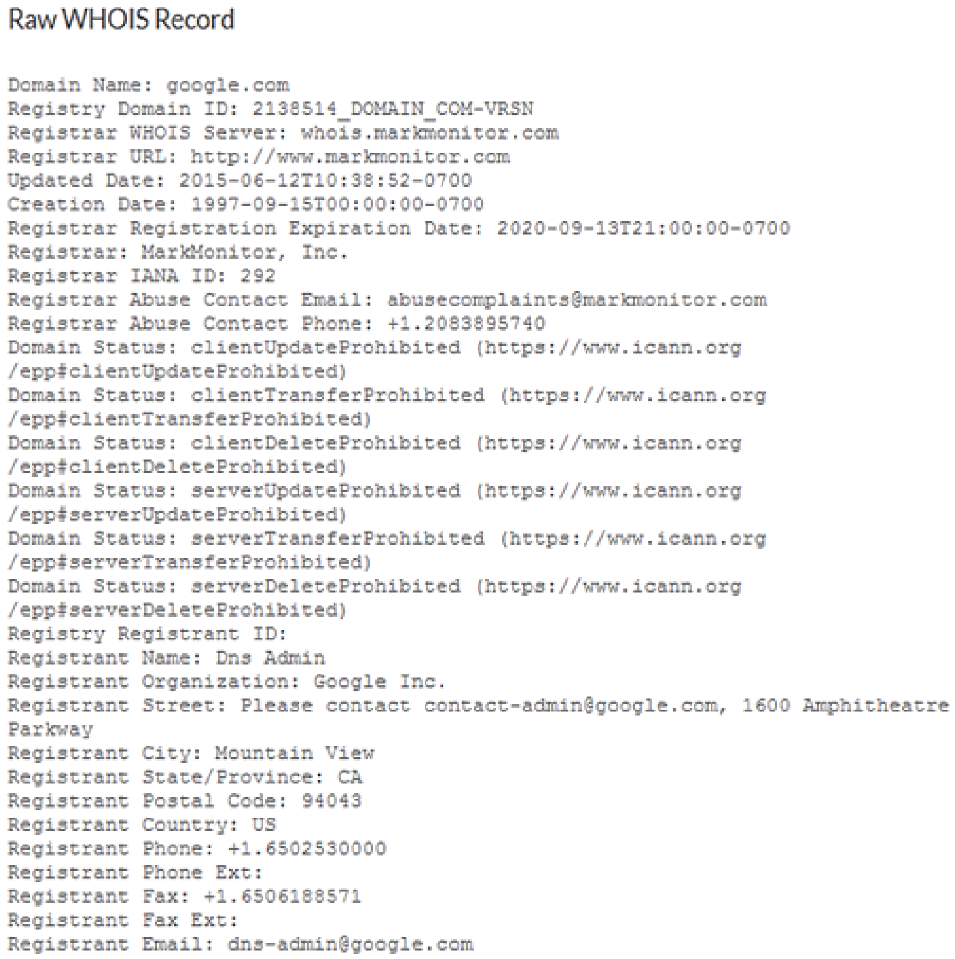
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\           nslookup 109.120.206.87
Server:
Address:

Name:    cache.google.com
Address:  109.120.206.87


C:\Users\
```

Websites for reverse DNS Lookup:
https://remote.12dt.com/
http://www.ipaddressguide.com/dnslookup
https://mxtoolbox.com/ReverseLookup.aspx
http://dnsgoodies.com/
http://www.dnsqueries.com/en/reverse_lookup.php

WHOIS lookup

WHOIS is a searchable database that contains information about every domain owner. The following information can be obtained from a WHOIS search: registrar, WHOIS server, nameservers, registration date, expiration date, registrant name, email address, IP address, telephone number. The Internet Corporation for Assigned Names and Numbers (ICANN) ensures all domains have valid WHOIS information.

You can retrieve this information via various WHOIS domain lookup systems, but it would perhaps be best if you start with the database on the ICANN's website. Linux or Mac users can use the following command in shell to perform a WHOIS search: whois domain name.



Raw WHOIS Record

```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2015-06-12T10:38:52-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org
/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org
/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org
/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org
/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org
/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org
/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Dns Admin
Registrant Organization: Google Inc.
Registrant Street: Please contact contact-admin@google.com, 1600 Amphitheatre
Parkway
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6502530000
Registrant Phone Ext:
Registrant Fax: +1.6506188571
Registrant Fax Ext:
Registrant Email: dns-admin@google.com
```

Sometimes WHOIS information is not available because some organizations specialize in offering private WHOIS registration. This is a method which replaces the domain owner information with their own.

Intelligence Gathering Tools /examples/

Netcraft – a free online tool specializing in gathering information on webservers, which covers both the server and client side technologies. Available at http://toolbar.netcraft.com/site_report/ (type the domain name).

MetaGoofil (python-based) – a metadata collection tool that searches the Internet for metadata related to your target. It is built on Kali Linux (so you can use it with Linux), it is also compatible with Windows. Similar tools for extracting metadata from a file (word/pdf/image) and displaying the results in formats such as HTML, XML, JSON, GUI, etc.: FOCA (GUI-based), meta-extractor, ExifTool (Perl-based).

Threatagent – another web-based tool for which you need to sign up at https://www.trustedsec.com/march-2013/threat-agent-a-smart-profiler-for-us-penetration-testers/ and type in the domain name subject to your reconnaissance aspirations. In the end, the drone extracts all the information you have requested and submits it to you in the form of a thorough report, which comprises IP address range, email address, the point of contact, etc.

Conclusion

As you can see, there are so many methods and resources that the penetration testers have at their disposal to execute the Intelligence Gathering – one of the most significant phases of the penetration testing process as a whole. Whoever attaches some importance to his cybersecurity, therefore, should at least know what information is publicly available about him and his business. Supposedly, when you know what may be used against you, the probability of negative events happening because of this information decreases a lot. In the end, that is the main goal of penetration testing.

Reference List

Acunetix. *What is Google Hacking?* Available at https://www.acunetix.com/websitesecurity/google-hacking/ (12/06/2016)

Czumak, M. (2014). *Passive Reconnaissance*. Available at http://www.securitysift.com/passive-reconnaissance/ (12/06/2016)

fr4nc1stein (2015). Google Dorks: An Easy Way of Hacking. Available at https://www.cybrary.it/0p3n/google-dorks-easy-way-of-hacking/ (12/06/2016)
Hack Cave. *The Basics of Penetration Testing*. Available at http://www.hackcave.net/2015/11/the-basics-of-penetration-testing.html(12/06/2016)

Gianchandani, P. (2011). *DNS Hacking (Beginner to Advanced).* Available at http://resources.infosecinstitute.com/dns-hacking/ (12/06/2016)

Google Hacker (2015). *Using Google as a website vulnerability scanner*. Available at http://www.ghackingdb.com/using-google-as-a-website-vulnerability-scanner/(12/06/2016)

Gupta, T. (2010). *5 penetration test tools to secure your network.* Available at www.computerweekly.com/tip/5-penetration-test-tools-to-secure-your-network(12/06/2016)

n00bs. *Intelligence Gathering*. Available at https://n00bpentesting.wordpress.com/lessons/ptes-101/intelligence-gathering/ (12/06/2016)

Octogence Technologies Pvt Ltd. *Importance of Reconnaissance in Pentesting*. Available at http://octogence.com/blog/reconnaissance/ (12/06/2016)

Rouse, M. (2005). *Forward DNS lookup*. Available at http://searchnetworking.techtarget.com/definition/Forward-DNS-lookup(12/06/2016)

Rumy, S. (2016). *Enumerating DNS records with DNSenum Tool in Kali Linux.* Available at http://rumyittips.com/enumerating-dns-records-with-dnsenum-tool-in-kali-linux/ (12/06/2016)

Tech-FAQ (2016). *Reverse DNS.* Available at http://www.tech-faq.com/reverse-dns.html (12/06/2016)

Tech-FAQ (2016). *How to Perform a DNS Lookup*. Available at http://www.tech-faq.com/how-to-perform-a-dns-lookup.html (12/06/2016)

True Demon (2015). *The Hacker Ethos*. Available at https://books.google.bg/books?id=-xhPCwAAQBAJ&pg=PT180&lpg=PT180&dq=eavesdropping+information+gathering&source=bl&ots=wYqDq-XtpT&sig=uYOpP8XI9-IVgm_DJZbCWqIxgGI&hl=bg&sa=X&ved=0ahUKEwiqm-W4vKrNAhUDtBQKHZkoAus4ChDoAQgzMAI#v=onepage&q=eavesdropping%20information%20gathering&f=false(12/06/2016)

Wing (2014). *15 Penetration Testing Tools-Open Source*. Available at http://securitywing.com/15-penetration-testing-tools-open-source/ (12/06/2016)

Vines, R. (2016). *Penetration testing reconnaissance* — Footprinting, scanning and enumerating. Available at http://searchitchannel.techtarget.com/tip/Penetration-testing-reconnaissance-Footprinting-scanning-and-enumerating (12/06/2016)

Webster (2016). Google Dorks : How to Use Google for Hacking. Available at http://www.hacoder.com/2016/01/google-dorks-how-to-use-google-for-hacking/(12/06/2016)

http://www.pentest-standard.org/index.php/Intelligence_Gathering (12/06/2016)

www.webhostingbuzz.com (2013).

What is a WHOIS Search. Available at http://www.webhostingbuzz.com/wiki/what-is-whois-search/ (12/06/2016)

From <https://resources.infosecinstitute.com/penetration-testing-intelligence-gathering/>

Network Topology

Sunday, December 23, 2018 1:44 AM

1. Introduction

Whenever we're doing a penetration test, it's good to figure out the topology of the network we're testing. We can't figure out the whole topology, because we don't have access to their internal network, but even if we manage to figure out part of the topology it's pretty cool.

But if we want to do that, we must have a pretty good understanding of what type of technology is usually implemented; thus we need to have at least a basic understanding of the following topics: switches, routers, IDS/IPSs, firewalls, VPNs, DMZs, VLANs, etc. This isn't such a small requirement.

First we must describe what all of those things are. For those of you who already know at least something about those topics, it'll be just a quick refresh, but if you've never encountered those, you should probably read more comprehensive material.

2. Networking Internals

Switch: A network switch or switching hub is a computer networking device that connects network segments or network devices [1]. We should remember that a network switch is operating at layer 2 OSI/ISO model (some of them also know about layer 3, but let's forget that for now). You should take a look at the Cisco switches as they are quite popular in larger networks.

Router: A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the "traffic directing" functions on the Internet [2]. The router is operating at layer 3 OSI/ISO, which means it is capable of doing NAT. NAT is a network address translation, translating WAN IPs into LAN IPs, so the packets can be routed though the internal network.

IDS: An intrusion detection system can be software-based or hardware-based and is used to monitor network packets or systems for malicious activity and do a specific action if such activity is detected. Usually, if malicious activity is detected on the network, the source IP of the malicious traffic is blocked for a certain period of time, and all of the packets from that IP address will be rejected. More about this can be read here: http://resources.infosecinstitute.com/packet-filtering/.

IPS: The intrusion prevention system is basically an upgrade of the intrusion detection system. Where the IDS is used to detect and log the attack, the IPS is used to detect, block and log the attack. The IPS systems are able to prevent certain attacks while they are happening. There are multiple versions of IPS systems, but we won't describe them in detail, since they are the same as with IDS systems, with the exception that all of the types of IPS system also prevent the attack from continuing. The types of IPS systems are: NIPS, HIPS, WIPS, NDA. More about this can be read here: http://resources.infosecinstitute.com/packet-filtering/.

Firewall: A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted. More about this can be read here: http://resources.infosecinstitute.com/packet-filtering/.

VPN: A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. A VPN provides security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network. VPNs can connect individual users to a remote network or connect multiple networks together [3]. When the network of a particular company is very big, not all of the hardware can usually be located at the same geographical place. But those hardware devices should nevertheless be part of the same network. So even if those network devices are connected to the Internet half a world away with a different ISP, they still need to be part of the same network. Let’s take a look at a simple example: if a company is dealing with computer hardware sells, they probably have shops all around the country (whatever country) and even in multiple countries. In order to keep those devices part of the same network even though their Internet is provided from different ISPs, the VPNs are used. Thus, through VPNs, users are able to access remote resources as if they were part of the same local network.

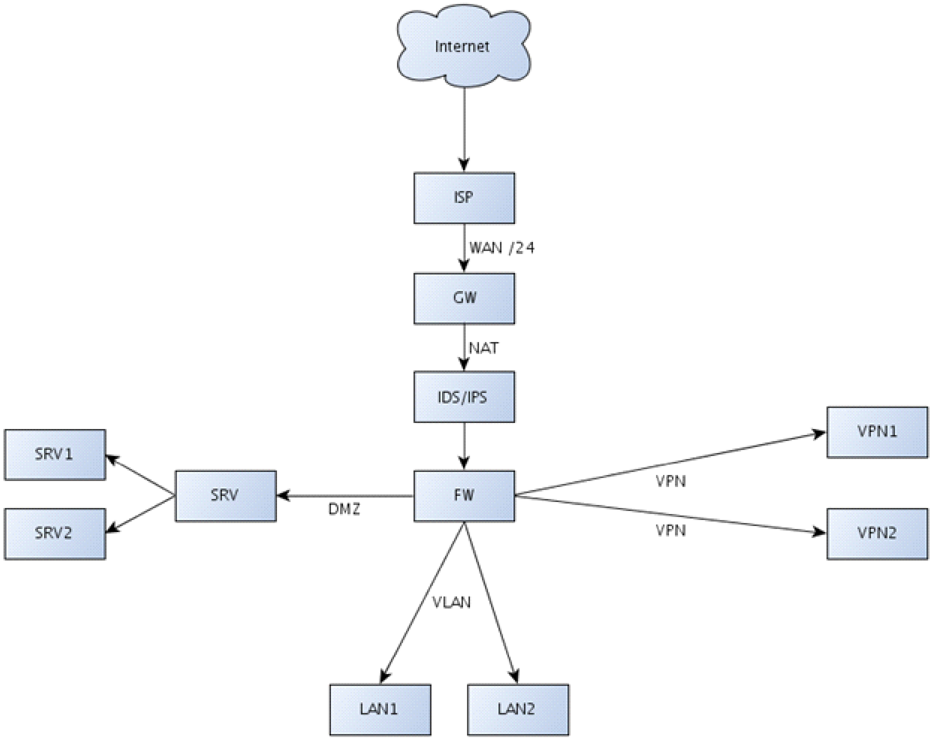
DMZ: DMZ is a physical or logical subnetwork that contains and exposes an organization’s external-facing services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization’s local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network [4]. We need to put only the servers that should be accessible to the world wide web into the DMZ. Thus, access to the servers in the DMZ zone will be allowed, but any other servers which are part of the same network but not in a DMZ will be hidden. The servers in the DMZ zone also don’t have access to the rest of the internal network, so even if a breach happens, the attacker will only be able to compromise the servers in the DMZ itself.

VLAN: VLAN is a concept of partitioning a physical network, so that distinct broadcast domains are created. This is usually achieved on switch or router devices. Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if not on the same network switch [5]. VLANs can be used to set up a virtual LAN, where we don’t have to physically relocate the devices, which is really good in virtualized environments. But let’s face it, almost every company today uses a virtualized networking setup.

3. Presenting a Network Topology

Here we’ll present a common network topology that can be seen in the picture below. I would like feedback on the picture presented. If you use a different topology can you please write a sentence or two about it so we can gather knowledge about different set-ups. I think various start-up companies can gain by that, because we can present the picture of different topologies, giving them different options to choose from, based on their requirements.

The topology below presents the way I see the network should be organized for a middle-sized company that uses /24 IP range.



We can see the network topology of a company with /24 IP range. We can see that at the entry point of the network there is a gateway followed by a IDS/IPS system and a firewall. Those are there to block known malicious attacks from attacking the systems in the internal network. After that we can see the **SRV** demilitarized zone, which holds all the servers that should be accessible to the outside world. There are also various local networks (LANs), where the VLANs can be in use (common if hardware virtualization is in place). But let’s not forget about the VPNs that can be present if the network is dispersed across multiple geographical locations.

4. Identify Network Topology: Simple Example

When identifying network topology of a company, we first need to determine its IP range. To identify the IP range of a Gentoo Linux foundation, we can use **nslookup** and **whois** tools as follows:

```
# nslookup gentoo.org
Server:        84.255.209.79
Address:       84.255.209.79#53
Non-authoritative answer:
Name:   gentoo.org
Address: 89.16.167.134
# whois 89.16.167.134
% Information related to '89.16.167.128 - 89.16.167.143'
inetnum:       89.16.167.128 - 89.16.167.143
status:        ASSIGNED PA
tech-c:        BYT2-RIPE
descr:         Gentoo Linux (www.gentoo.org)
netname:       BYTEMARK-GENTOOLINUX
country:       GB
admin-c:       BYT2-RIPE
source:        RIPE # Filtered
mnt-by:        MNT-BYTEMARK
```

We can see that the Gentoo Linux has an IP range of 89.16.167.128 – 89.16.167.143, which can be represented with a CIDR 89.16.167.128/28. This can by calculated manually by hand or with an online tool accessible on a web page like this one.

We can also see that the Gentoo Linux is hosted at http://www.bytemark.co.uk, which we need to further investigate. To identify the ASN number of the ByteMark hosting company, we can execute the whois command below:

```
# whois -h whois.cymru.com 89.16.167.134
AS      | IP              | AS Name
35425   | 89.16.167.134   | BYTEMARK-AS Bytemark Computer Consulting Ltd
```

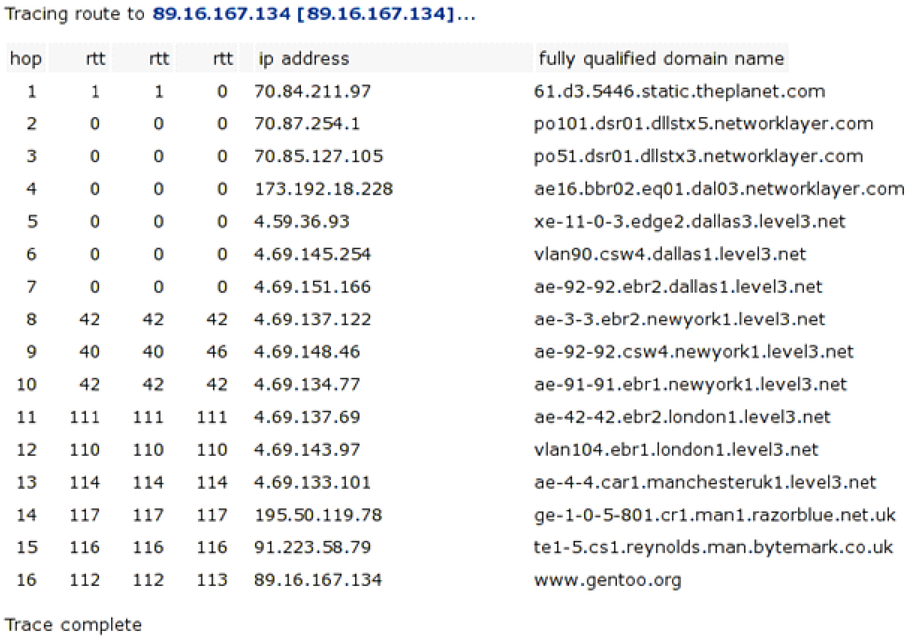
Cool, the ASN number of “BYTEMARK-AS Bytemark Computer Consulting Ltd” is **35425**. But we want to go further; we need to find out all IP addresses that are in the jurisdiction of ByteMark. We can again do this with whois command like this:

```
# whois -h whois.ripe.net -i origin -T route AS35425 | grep -w "route:" | awk '{print $NF}' | sort -n
5.153.224.0/21
46.43.0.0/18
46.43.35.0/24
80.68.80.0/20
80.68.80.0/21
80.68.88.0/21
89.16.160.0/19
91.223.58.0/24
212.110.160.0/19
212.110.177.0/24
213.138.96.0/19
```

Notice that we used the **AS35425** number, we learned in the previous step? Okay, so the Gentoo Linux IP range belongs in the 89.16.160.0/19 range.

The next thing is to **traceroute** the IP on the Gentoo Linux domain from different locations to find out the entry points.

The results of a traceroute from a web site http://centralops.net/ are presented below. We can see that the first node in the Bytemark hosting company is 91.223.58.79, which has direct access to the 89.16.167.134 that belongs to Gentoo. This is logical, because the Gentoo Linux doesn’t have its own autonomous system (AS), so the Bytemark should have direct access to its own hosts.

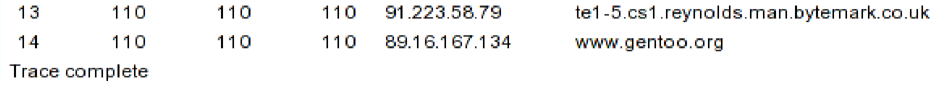


Tracing route to 89.16.167.134 [89.16.167.134]...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	1	1	0	70.84.211.97	61.d3.5446.static.theplanet.com
2	0	0	0	70.87.254.1	po101.dsr01.dllstx5.networklayer.com
3	0	0	0	70.85.127.105	po51.dsr01.dllstx3.networklayer.com
4	0	0	0	173.192.18.228	ae16.bbr02.eq01.dal03.networklayer.com
5	0	0	0	4.59.36.93	xe-11-0-3.edge2.dallas3.level3.net
6	0	0	0	4.69.145.254	vlan90.csw4.dallas1.level3.net
7	0	0	0	4.69.151.166	ae-92-92.ebr2.dallas1.level3.net
8	42	42	42	4.69.137.122	ae-3-3.ebr2.newyork1.level3.net
9	40	40	46	4.69.148.46	ae-92-92.csw4.newyork1.level3.net
10	42	42	42	4.69.134.77	ae-91-91.ebr1.newyork1.level3.net
11	111	111	111	4.69.137.69	ae-42-42.ebr2.london1.level3.net
12	110	110	110	4.69.143.97	vlan104.ebr1.london1.level3.net
13	114	114	114	4.69.133.101	ae-4-4.car1.manchesteruk1.level3.net
14	117	117	117	195.50.119.78	ge-1-0-5-801.cr1.man1.razorblue.net.uk
15	116	116	116	91.223.58.79	te1-5.cs1.reynolds.man.bytemark.co.uk
16	112	112	113	89.16.167.134	www.gentoo.org

Trace complete

Let’s try to run a few more traceroutes from different locations. The results of a traceroute from a web site http://network-tools.com/ are presented below.



```
 13        110        110        110    91.223.58.79        te1-5.cs1.reynolds.man.bytemark.co.uk
 14        110        110        110    89.16.167.134       www.gentoo.org
Trace complete
```

We can see the same results as above, the connection to 89.16.167.134 is going through 91.223.58.79. If we run the traceroute from a few more locations we can get a different result, because the packets would be routed from a different Bytemark router with a different IP.
We can see that since the Gentoo Linux topology really isn't that complicated, because they don't have their own ASN. And their hosting provider Bytemark really shouldn't have a filter or IDS/IPS system in place, because it's the job of the end customer to apply those. If the hosting provider would filter the packets destined to the ending IP address (whatever they are running; http, ssh, ftp, etc), they would need to look at the packets themselves and accept/deny them, which can cause a lot of problems. For example, let's say I'm connecting to www.gentoo.org, but the Bytemark's hosting filter decides that it will not let my packets through (for whatever reason). Can you see the problem there? It's not the Bytemark's decision what packets are going to Gentoo's website and they shouldn't decide to allow/block the connections.

5. Conclusion

We've seen how can we get a basic topology of a really simple company, but often the task is not that simple, because there are multiple filters, IDS/IPS systems in place that can block our requests. Usually the traceroute itself doesn't print all the hosts on the way to the target, because when the packet is entering the customer's network, it can be checked, filtered or even blocked.

References:

[1] Network switch, Wikipedia, accessible on http://en.wikipedia.org/wiki/Network_switch.
[2] Router (computing), Wikipedia, accessible on http://en.wikipedia.org/wiki/Router_(computing).
[3] Virtual private network, Wikipedia, accessible on http://en.wikipedia.org/wiki/Virtual_private_network.
[4] DMZ (computing), Wikipedia, accessible on http://en.wikipedia.org/wiki/DMZ_(computing).
[5] Virtual LAN, Wikipedia, accessible on http://en.wikipedia.org/wiki/Virtual_LAN.

From <https://resources.infosecinstitute.com/network-topology/>