NASA hw5

B04902045 孫凡耘

May 12, 2017

Network Administration

DHCP

DHCP Snooping is an option to prevent rogue DHCP servers on the Lan segment.DHCP snooping can ensure IP integrity on a Layer 2 switched domain. It works with information from a DHCP server to:

- Track the physical location of hosts.
- Ensure that hosts only use the IP addresses assigned to them.
- Ensure that only authorized DHCP servers are accessible.(*)

Commands(example):

```
configure dhcp snooping on your vlan
$ Ip dhcp snooping
$ Ip dhcp snooping vlan 1
for trusted servers
$ Int fa2/10
$ Ip dhcp snooping trust
```

DNS

1

No computer will query your computer cause they are not set to query the dns server(Unless they change the configuration manually). Usually, the default is set to well-known DNS servers such as Google public dns or openDNS.

2

Domain:

```
in-addr.arpa
```

When DNS is used to find something on the internet, it always starts at the least specific(後面開始看). So in names, the least specific part comes last, but in IP addresses, it comes first，所以要 revert ip addresses.

3

Whois lookup:
webpage tool: `http://whois.domaintools.com/icann.org`
Email: domain-admin@icann.org

4

When you update the nameservers for a domain, it may take up to 24-72 hours for the change to take effect. This period is called DNS propagation.

In other words, it is a period of time ISP (Internet service provider) nodes across the world take to update their caches with the new DNS information of your domain.

Due to DNS caches of different levels, after the nameservers change, some of your visitors might still be directed to your old server for some time, whereas others can see the website from the new server shortly after the change.
reference: `https://www.namecheap.com/support/knowledgebase/article.aspx/9622/10/dns-propagation--explained`

A zone file is a sequence of entries for resource records. Each line is a text description that defines a single resource record (RR). The description consists of several fields separated by white space (spaces or tabs) as follows:

```
name    ttl     record class    record type     record data
```

When a caching (recursive) nameserver queries the authoritative nameserver for a resource record, it will cache that record for the time (in seconds) specified by the TTL.
3600 ==> 1 hour

5

An "open DNS resolver" is a DNS server that's willing to resolve recursive DNS lookups for anyone on the internet.
What problem may is pose ?
Short answer: attacker can make use of the open DNS resolver to perform a DDos attack.
The way this attack works is pretty simple - because your server will resolve recursive DNS queries from anyone, an attacker can cause it to participate in a DDoS by sending your server a recursive DNS query that will return a large amount of data, much larger than the original DNS request packet. By spoofing (faking) their IP address, they'll direct this extra traffic to their victim's computers instead of their own, and of course, they'll make as many requests as fast as they can to your server, and any other open DNS resolvers they can find. In this manner, someone with a relatively small pipe can "amplify" a denial of service attack by using all the bandwidth on their pipe to direct a much larger volume of traffic at their victims. reference: `https://serverfault.com/questions/573465/what-is-an-open-dns-resolver-and-how-can-i-protect-my-server-from-being-misused`

System Administration

1

yum upgrade forces the removal of obsolete packages, while yum update may or may not also do this. The removal of obsolete packages can be risky, as it may remove packages that you use.

2

yum upgrade is the same as the update command with the –obsoletes flag set.

3

yum remove will remove only that package and not all the dependencies.
yum autoremove will remove unneeded dependencies from that installed package.

4

If you don't want packages to be deleted, as they were installed as dependency before, you must mark them as installed:

```
$ yum install #package
```

5

```
$ yum search vim
```

6

```
$ yum provides nfsstat
```

7

```
$ repoquery --tree-requires <My-Package>
```

8

PyPI
pros: convenience, 可以安裝很多人 contriute 的 repository(PyPI is a third-party software repositories)
cons: security issue, PyPI does not prevent people from uploading malware.

CentOS 7 repository
pros: 官方的 repo 對 security 有把關, 像第 10 題, 如果缺少不同程式語言的

dependency(ex: gcc), yum install 可以下參數幫你一起裝起來但 pip 不能
cons: 官方的 repo 資源比較少，可能也找不到最新的版本之類的 (造成類似第 10 題的 version conflict)

9

The command

```
$ sudo yum remove -y python-jinja2
```

yields a lot of error messages, basically saying file or directory not found(也就是已經被移除了找不到)
The reason of this is that jinja2 is uninstalled by pip previously.

10

View next page