ComputerNetworkingNotes

Reconnaissance attacks, Tools, Types, and Prevention

This tutorial explains reconnaissance attacks in detail. Learn what reconnaissance attacks are, types of reconnaissance attacks, how reconnaissance attacks are performed, and how to prevent a network from reconnaissance attacks.

What is a reconnaissance attack?

A reconnaissance attack is a type of security attack that an attacker uses to gather all possible information about the target before launching an actual attack. An attacker uses a reconnaissance attack as a preparation tool for an actual attack.

Types of reconnaissance attacks

There are three types of reconnaissance attacks. These are social, public, and software. Let's discuss these types in detail.

Social reconnaissance attacks

In this type of attack, a hacker uses social engineering to gather information about the target. Users share a lot of personal and business information on social networking sites. A hacker can use social networking sites to gather information about the target. For example, if the target is a company, the hacker can use social networking sites to reveal information about the company's employees.

A hacker can use honey trap techniques to lure an employee. Once the employee accepts the friend request of the hacker, the hacker starts the next step. In the next step, the hacker convinces the employee to reveal information about his business. For example, the hacker may provide technical support to the employee on his project. Or the hacker may offer some monetary reward for disclosing information about the company.

To reduce social reconnaissance attacks, a company must train its employees about what information they cannot share with others within and outside the company. Employees should never share sensitive information on any social platform. If an employee shares any confidential information with unknown persons or outside users, the company must take appropriate action against the employee.

Public reconnaissance attacks

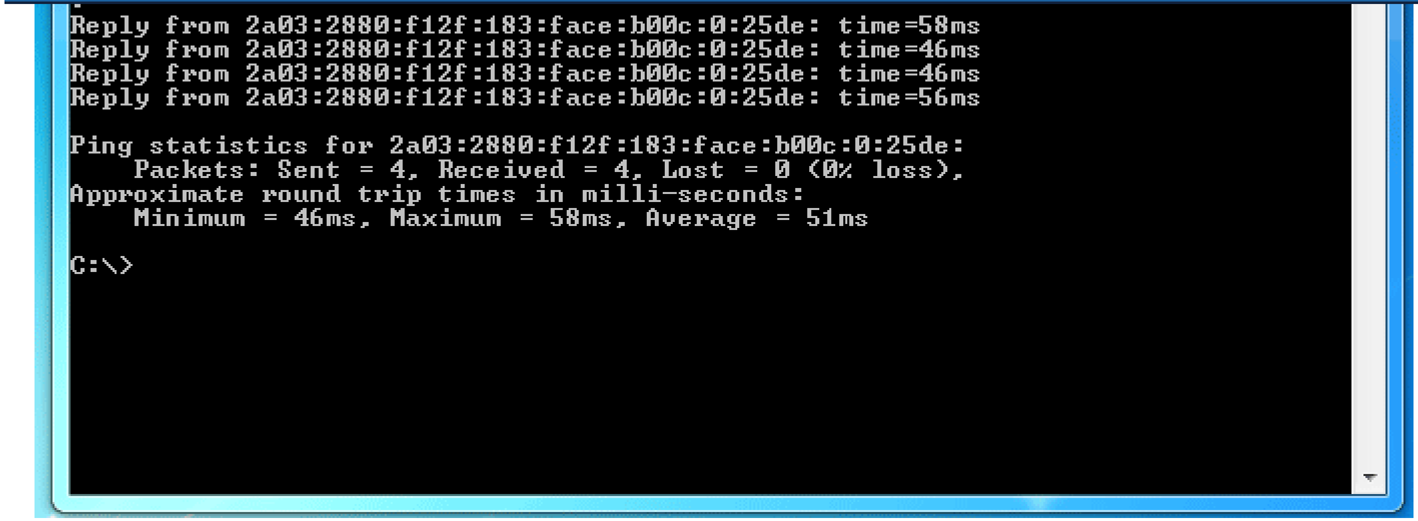
information to find vulnerabilities in the company's network.

To mitigate public reconnaissance attacks, companies should not share confidential information on public platforms. For business requirements, if a company wants to share information about its infrastructure, instead of sharing exact hardware information, it should share generic information. Generic information will fulfill the business requirement. From generic information, a hacker can't guess the product information. For example, if a company uses the Cisco Firepower 4100 Firewall, it may publish that we use the Cisco Firewall.

Software reconnaissance attacks

In this type of attack, a hacker uses software tools to gather information about the target. Operating systems and software packages include many tools and utilities for debugging and troubleshooting. A hacker can use them to collect information about the network and its resources. For example, a hacker can use the **nslookup** command to perform a DNS lookup. The **nslookup** command resolves an IP address from a fully qualified domain name. Once the hacker knew the domain name of the business, the hacker can use the whois database to reveal detailed information about domain owners, mail servers, contact information, authoritative DNS servers, etc.

In the next step, the hacker can use the **ping** command. The **ping** command sends packets to the target host. If the target host is live, the host replies to the packets. Reply packets verify that the target host is live. The following image shows the sample output of the **ping** command.

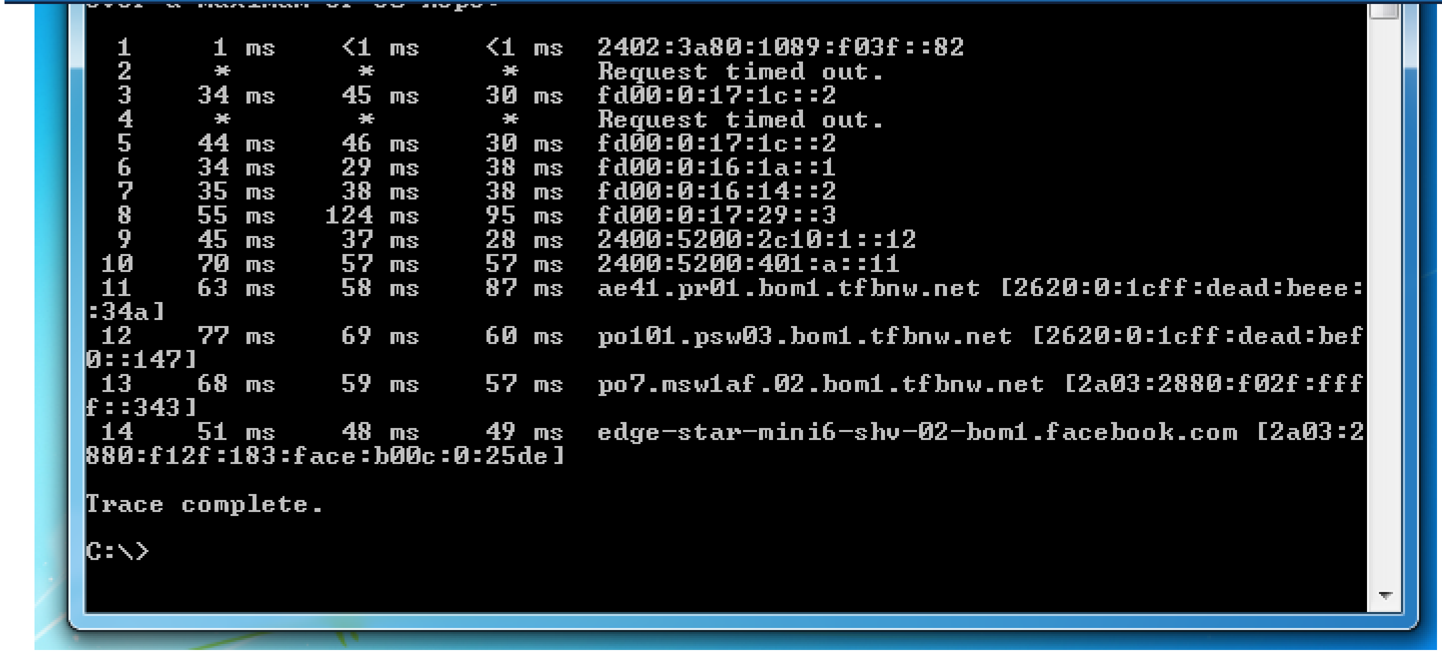


```
Reply from 2a03:2880:f12f:183:face:b00c:0:25de: time=58ms
Reply from 2a03:2880:f12f:183:face:b00c:0:25de: time=46ms
Reply from 2a03:2880:f12f:183:face:b00c:0:25de: time=46ms
Reply from 2a03:2880:f12f:183:face:b00c:0:25de: time=56ms

Ping statistics for 2a03:2880:f12f:183:face:b00c:0:25de:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 58ms, Average = 51ms

C:\>
```

In addition to the **ping** command, the hacker can also use the **tracert** command. The **tracert** command prints the path that packets use to reach the destination device. With the help of the **ping** command and the **tracert** command, a hacker can create a visual map of the target network. The following image shows an example of the **tracert** command.



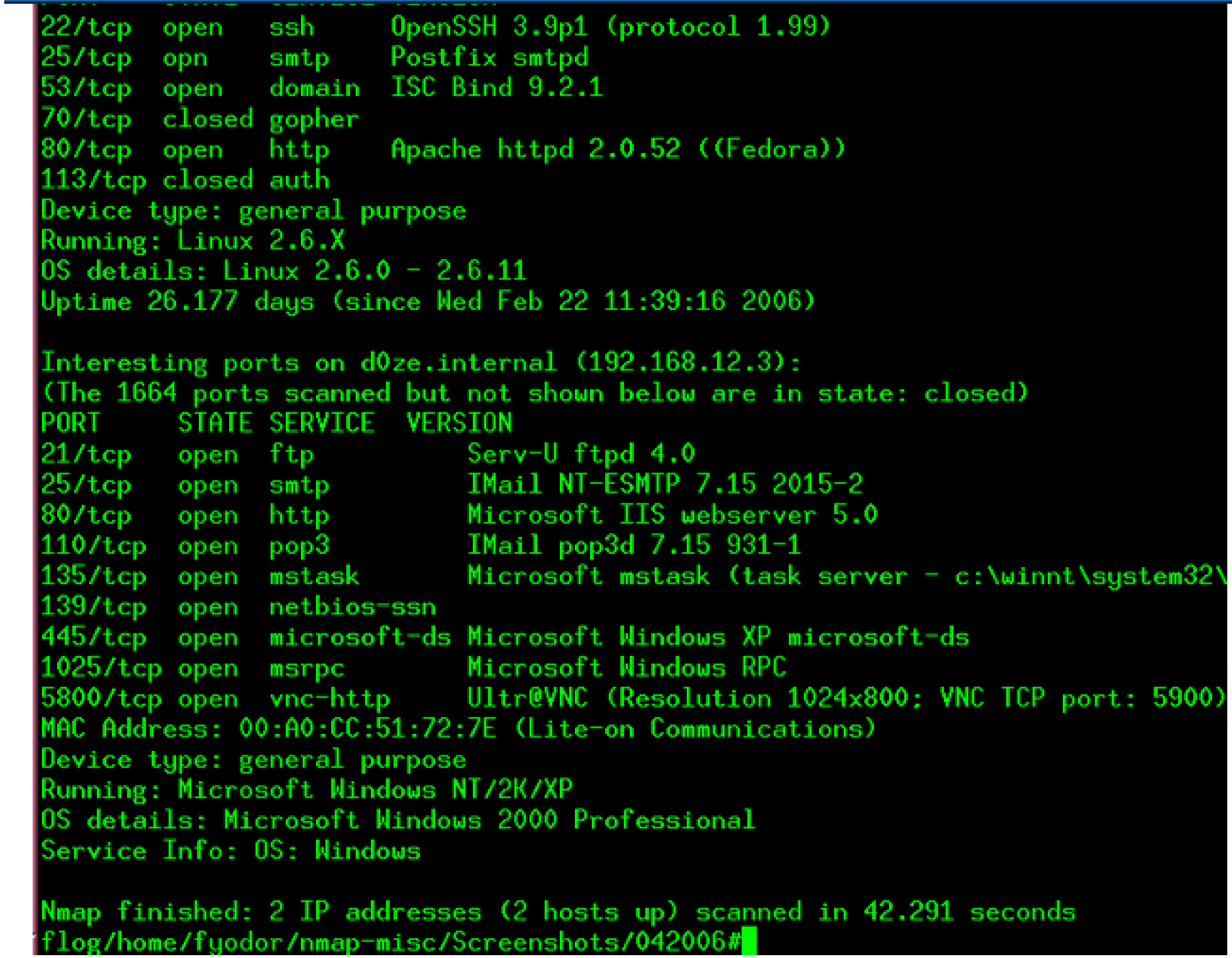
```
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  2402:3a80:1089:f03f::82
  2     *        *        *     Request timed out.
  3    34 ms    45 ms    30 ms  fd00:0:17:1c::2
  4     *        *        *     Request timed out.
  5    44 ms    46 ms    30 ms  fd00:0:17:1c::2
  6    34 ms    29 ms    38 ms  fd00:0:16:1a::1
  7    35 ms    38 ms    38 ms  fd00:0:16:14::2
  8    55 ms   124 ms    95 ms  fd00:0:17:29::3
  9    45 ms    37 ms    28 ms  2400:5200:2c10:1::12
 10    70 ms    57 ms    57 ms  2400:5200:401:a::11
 11    63 ms    58 ms    87 ms  ae41.pr01.bom1.tfbnw.net [2620:0:1cff:dead:beee:
:34a]
 12    77 ms    69 ms    60 ms  po101.psw03.bom1.tfbnw.net [2620:0:1cff:dead:bef
0::147]
 13    68 ms    59 ms    57 ms  po7.msw1af.02.bom1.tfbnw.net [2a03:2880:f02f:fff
f::343]
 14    51 ms    48 ms    49 ms  edge-star-mini6-shv-02-bom1.facebook.com [2a03:2
880:f12f:183:face:b00c:0:25de]

Trace complete.

C:\>
```

In the next step, the hacker can use port scanners to detect running services on the target host. To scan services, the hacker can use **nmap** scanner. The following image shows a sample output of the **nmap** port scanner.



```
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

To mitigate software reconnaissance attacks, an administrator can use the following techniques: -

- Can disable all unused ports on servers
- Can use the masking service to hide sensitive information on the **whois** database