OSI Network Protocol Stack

	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Transport
3	Network	Internet
2	Data link	Data link
1	Physical	Physical

Port Scanning—Nmap

To find services (*exploitable communication channels*) running on your machine.

TCP header

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td></tr>
<tr><td colspan="16">Source port</td><td colspan="16">Destination port</td></tr>
<tr><td colspan="32">Sequence number</td></tr>
<tr><td colspan="32">Acknowledgement number (1 + last byte # recvd)</td></tr>
<tr><td colspan="4">Hdr len</td><td colspan="6">Reserved</td><td colspan="6">Code</td><td colspan="16">Window</td></tr>
<tr><td colspan="16">Checksum</td><td colspan="16">Urgent pointer</td></tr>
<tr><td colspan="24">Options if any</td><td colspan="8">padding</td></tr>
<tr><td colspan="32">DATA</td></tr>
</table>

CODE is 6 bits, from left to right: URG, ACK, PSH, RST, SYN, FIN.

- TCP connect scanning. Can result in application-level logging.
- TCP SYN scanning aka Stealth mode. Leads to denial of service in many OSes. Could be logged.
- TCP FIN scanning.
- Fragmentation scanning. Split TCP header (SYN) into multiple packets.
- UDP ICMP port unreachable scanning. May be limited by the host's error limit rate.
- Ping sweeps.
- IP Protocol scanning.
- Xmas tree scan: FIN|URG|PSH.

Remote OS detection via TCP/IP Stack Fingerprinting

Why?

- Many security holes dependent on OS version.
- Scan a network for (OS,svc) pairs and wait for next exploit.
- Social engineering.

How?

- Just telnet to the machine.
- Telnet to the ftp port.
- DNS host info record.
- snmpwalk.

Basically, look for things that are different among OSes and write a probe for the difference.

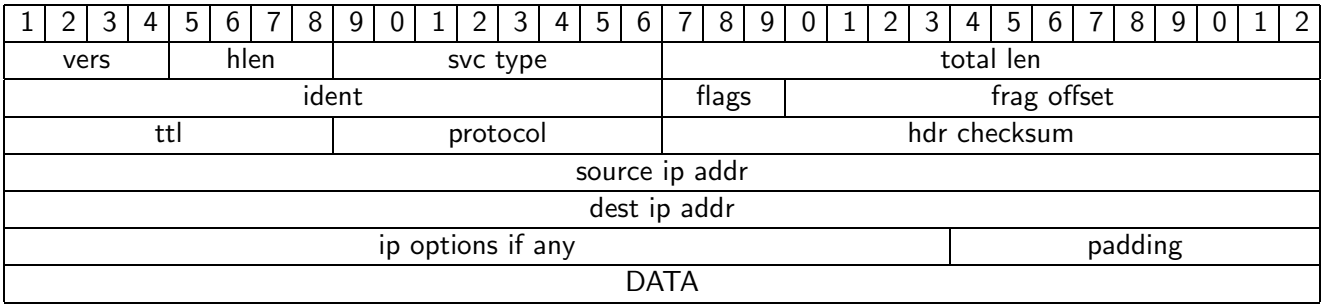
- FIN scan to known open port. Windows boxes will send RST back.
- BOGUS flag returned on some Linuxes. (SYN+BOGUS) returns (ACK + BOGUS).
- ISN sampling. Some always use the same ISN! Random increments, true "random", time-dependent model,. . .
- Don't Fragment bit in the IP header.
- TCP Initial window size (during handshake or on RST packets). AIX = 16165!
- ACK value on RST returned on a FIN|PSH|URG sent to a closed port?
- ICMP error message rate. Some systems such as Linux will rate limit the returned error messages.
- ICMP message quoting size. How much of the offending packet is returned. Only header+64 bits returned or more or the whole packet.

- TOS on ICMP port unreachables. Overlapping fragments for TCP.
- Fragmentation handling.
- TCP options, which ones supported, order of return,. . .

Examples of Nmap configuration

- `T5(DF=N%W=0%ACK=S++%Flags=AR%Ops=)` - SYN to a closed port.
- `T6(DF=N%W=0%ACK=O%Flags=R%Ops=)` - ACK to a closed port.

IP header



Software Forensics

Adapted from http://www.fish.com/tct/help-when-broken-into.

Reconstructing the past based on current evidence.

- Secure & Isolate. Simply disconnect the system from the network.
- Record the scene.
- Search for evidence. *Can you trust the tools*? [Reflections on Trusting Trust—Ken Thompson.]

Do you suspect that you've been broken into

Adapted from [HLK01, pg. 61].

- Web page defacement.
- Dramatic increase in disk space.
- High network usage.
- Promiscuous network interfaces.
- Contact from other administrators.
- Wiped or truncated logs.
- Strange processes running.
- Local users have had remote accounts cracked.
- Things just "seem funny".

Have you been broken into–Use logging effectively

Adapted from the CERT Intruder Detection Checklist.

- Connections from unusual locations.
  - utmp, man(5). Binary file that contains a record for every active *tty* line i.e., information about who is currently using the system.

    ```
    -rw-rw-r--    1 root     utmp         6528 Mar 15 13:43 /var/run/utmp
    ```

    Used by *who, w, users, finger*.
  - wtmp. Keeps track of both logins and logouts.

    ```
    -rw-rw-r--    1 root     utmp        65664 Mar 18 02:07 /var/log/wtmp
    ```

    Used by *last*.

    ```
    ftp      ftpd945      csa.iisc.ernet.i Fri Mar  8 14:35 - 14:35  (00:00)
    reboot   system boot  2.4.7-10         Fri Mar  8 14:34         (6+20:03)
    s-kumar  pts/5                        Thu Mar  7 16:40 - 13:30  (20:50)
    ftp      ftpd2548     csa.iisc.ernet.i Thu Mar  7 14:08 - 14:08  (00:00)
    ```
  - lastb
  - Process Accounting. /var/log/pacct* on RH Linux. No command args and no cwd. Used by *lastcomm*.

    ```
    logrotate         S     root     ??         0.02 secs Mon Mar 18 04:02
    gzip                    root     ??         1.13 secs Mon Mar 18 04:02
    sh                      root     ??         0.01 secs Mon Mar 18 04:02
    accton            S     root     ??         0.00 secs Mon Mar 18 04:02
    ```
  - syslog man syslog, /etc/syslog.conf. (Facility, Level, Action)

    ```
    authpriv.*                                              /var/log/secure
    mail.*                                                  /var/log/maillog
    cron.*                                                  /var/log/cron
    *.emerg                                                 *
    news.=err                                               /var/log/news/news.err
    *.info;mail.none;news.none;cron.none                    /var/log/messages
    ```

    Facilities: authpriv, cron, daemon, kern, lpr, mail, news, user,...
    Level: emerg, alert, crit, err, warning, notice, info, debug.

    Mar 17 08:37:19 suk ftpd[24314]: ANONYMOUS FTP LOGIN FROM csa.iisc.ernet.in [144.16.67.8], anarchie@csa.iisc.ernet.in

  - tcpwrappers
  - Apache access log (/var/log/httpd/access_log*). What sites have been contacting and which files have been downloaded.
- Setuid and setgid files.

  find / -user root -perm -4000 -xdev -print
- Check system binaries for alteration – mods, content.
  Save them on a WORM device, on a different machine. Tripwire, AIDE, Nabou. Protecting modes are needed because:
  - Log files can be made readable.
  - System programs/startup scripts could be made writable.
  - Sticky bit could be unset to allow for symlink race condition attacks.
  - Writable setxid programs.
- Check for unauthorized use of network monitoring program.
- Examine all files run by "cron" and "at".
- Check /etc/inetd.conf (/etc/xinetd.conf) for unauthorized additions or changes. On kohinoor, a sample entry in inetd.conf is:

  ```
  ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
  ```

  The *nowait* specifies that inetd should spawn *tcpd* on receiving a connection and returning to listening on new connections on the ftp port, i.e., to *not wait* for tcpd to exit. The *wait* option is mostly for UDP based services.
- Check /etc/passwd for new accounts, accounts with no passwords, uid changes to existing accounts.
- Check network configuration files /etc/hosts.equiv, `~/.rhosts`, /etc/hosts.lpd. The format of entries in /etc/hosts.equiv is [+—-] [hostname] [username]. Ex:

nirvana	allow like-named users on nirvana to access localhost without password.
+nirvana	allow any user in nirvana access to access localhost without password.
+skumar	allow skumar from any host to any account on localhost (except root) without password.
-nirvana	always require password from nirvana.
+	allow any host/any user access to your system without password.

- Look for hidden or unusual files—'...', '.. ', '..^G' etc.
- Examine all machines on the local network.

What to do now?

Adapted from http://www.fish.com/tct/help-when-broken-into.

- Create a security policy.
  - No modem connections, wireless or otherwise.
  - No connection of non-Sun OSes on SWAN.
  - Regular password changes.
  - No compilation or running of outside untested programs.
- Install any and all vendor patches.
- Turn off all unneeded network services.
- Learn your system better.
- Turn on logging and accounting.
- Create a baseline.
- Regularly audit or at least examine your systems.

Future

- Keep your eyes open and learn from your mistakes.
- Keep good recoverable backups.

References

[HLK01] Brian Hatch, James Lee, and George Kurtz. *Hacking Linux Exposed: Linux Security Secrets & Solutions*. Osborne/McGraw-Hill, 2001.