

Security

Tools and tricks for computing in a
hostile environment

Most Important Rules

- 1) Know what's running on your machine
- 2) Don't run services you don't need
- 3) Keep your software updated
- 4) Log and monitor
- 5) React to threats with as much paranoia as policy will allow

Finding out what your machine is doing

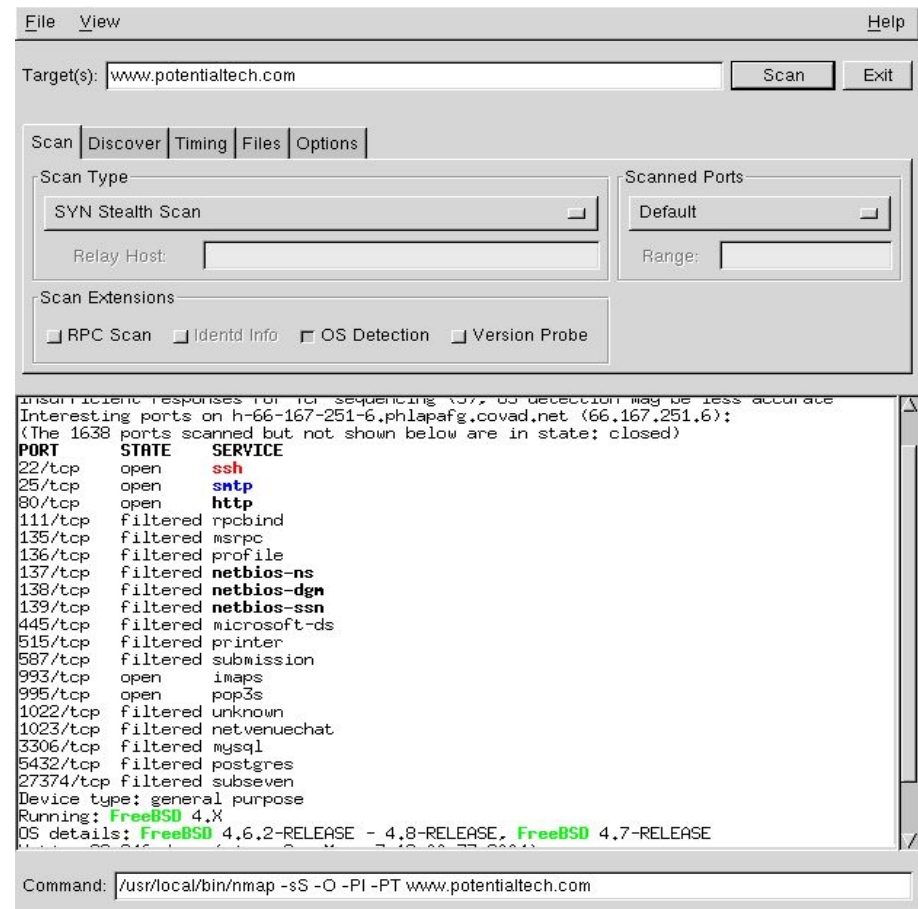
```
# netstat -ltp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp      0      0 *:32770                 *:                       LISTEN     3256/rpc.statd
tcp      0      0 *:32771                 *:                       LISTEN     -
tcp      0      0 localhost.localdo:32772 *:                       LISTEN     3388/xinetd
tcp      0      0 *:sunrpc                 *:                       LISTEN     3236/portmap
tcp      0      0 localhost.localdoma:ipp *:                       LISTEN     3345/cupsd
tcp      0      0 *:23000                  *:                       LISTEN     3427/ZideStore
tcp      0      0 *:14238                  *:                       LISTEN     3428/nhsd
```

/etc/rc?.d directories (or use distro-specific tool)

Check inetd/xinetd config

nmap

- Tool for scanning computers for listening ports.
- Use to inventory the servers running on a machine.
- Recommended to ensure that you've done step 1 & 2 completely.



```
insufficient responses for TCP sequencing (SYN) OS detection may be less accurate
Interesting ports on h-66-167-251-6.phlapafg.covad.net (66.167.251.6):
(The 1638 ports scanned but not shown below are in state: closed)
PORT      STATE      SERVICE
22/tcp    open       ssh
25/tcp    open       snmp
80/tcp    open       http
111/tcp   filtered  rpcbind
135/tcp   filtered  msrpc
136/tcp   filtered  profile
137/tcp   filtered  netbios-ns
138/tcp   filtered  netbios-dgm
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
515/tcp   filtered  printer
587/tcp   filtered  submission
993/tcp   open       imaps
995/tcp   open       pop3s
1022/tcp  filtered  unknown
1023/tcp  filtered  netvenuechat
3306/tcp  filtered  mysql
5432/tcp  filtered  postgres
27374/tcp filtered  subseven
Device type: general purpose
Running: FreeBSD 4.X
OS details: FreeBSD 4.6.2-RELEASE - 4.8-RELEASE, FreeBSD 4.7-RELEASE
Command: /usr/local/bin/nmap -sS -O -PI -PT www.potentialtech.com
```

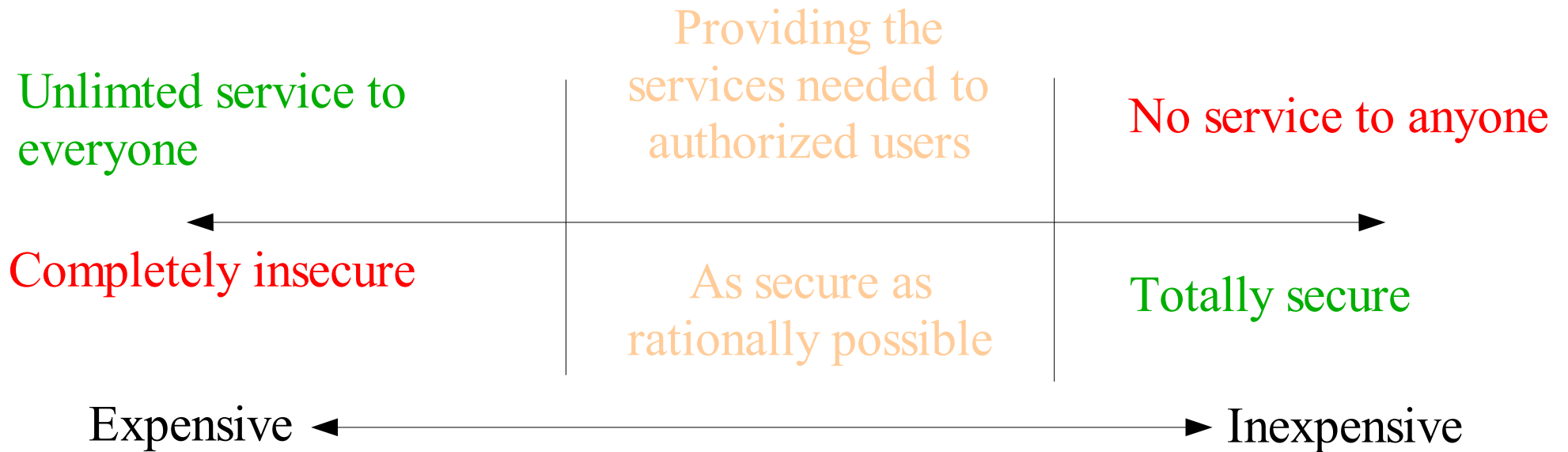
Some of the things attackers may be trying to accomplish
(or “how paranoid should you be”)

- 1) Prevent your server from doing its job (“Denial of Service”)
- 2) Get access to files on your computer
- 3) *Use your computer as a “zombie” to attack other computers
- 4) *Use your computer to relay spam
- 5) *Use your computer to play a prank that won't be tracable
- 6) *Use your computer as a distribution point for illegal software (“warez”) or worse

Keep software updated

- If a problem exists, take the time to fix it: never assume that nobody will notice.
- Subscribe to lists applicable to your distribution, example: `security@freebsd.org`, `announce@httpd.apache.org`
- Cert (<http://www.cert.org>) is a good place to keep up on general security issues.

The war between service and security



Weak passwords

Presence of a weak password can invalidate all security efforts.

cracklib: runs a number of checks against a suggested password to ensure that it is strong enough. Most distros are already using this in an advisory fashion. See configuration in `/etc/pam.d`

Filtering Packets

A packet filter is a program that allows you to accept or deny (i.e. Filter) network traffic based on criteria.

Linux's IPCHAINS:

```
ipchains -A input deny -s 10.57.1.14
```

FreeBSD's IPFW:

Starting ruleset:

```
ipfw add 65000 pass all from any to any
```

Adding a quick block from an attacker:

```
ipfw add 100 deny all from 10.57.1.14 to me
```

Reaction: what to do when it happens

Two common scenerios:

- 1) Most common (if you've done a good job securing things): you notice a break-in attempt that is failing
This is pre-emptive defense: learn from this failed attack, what can you do to improve defense/monitoring?
- 2) Much worse: you notice that a break-in attempt succeeded
This is pure reaction: you've got to assess the damage and quickly get things working again

Practice writing packet filter rules prior to something going wrong, have the packet filter you prefer to use installed and configured **before** anything happens!

Know your service policy and ensure that your reaction is in line with your service policy!

Monitoring: Watch for symptoms

- Unusual amounts of network traffic
- Unusual types of network traffic
- Machines suddenly running slower than usual
- Processes that you don't recognize
- Strange log entries (not always errors!)

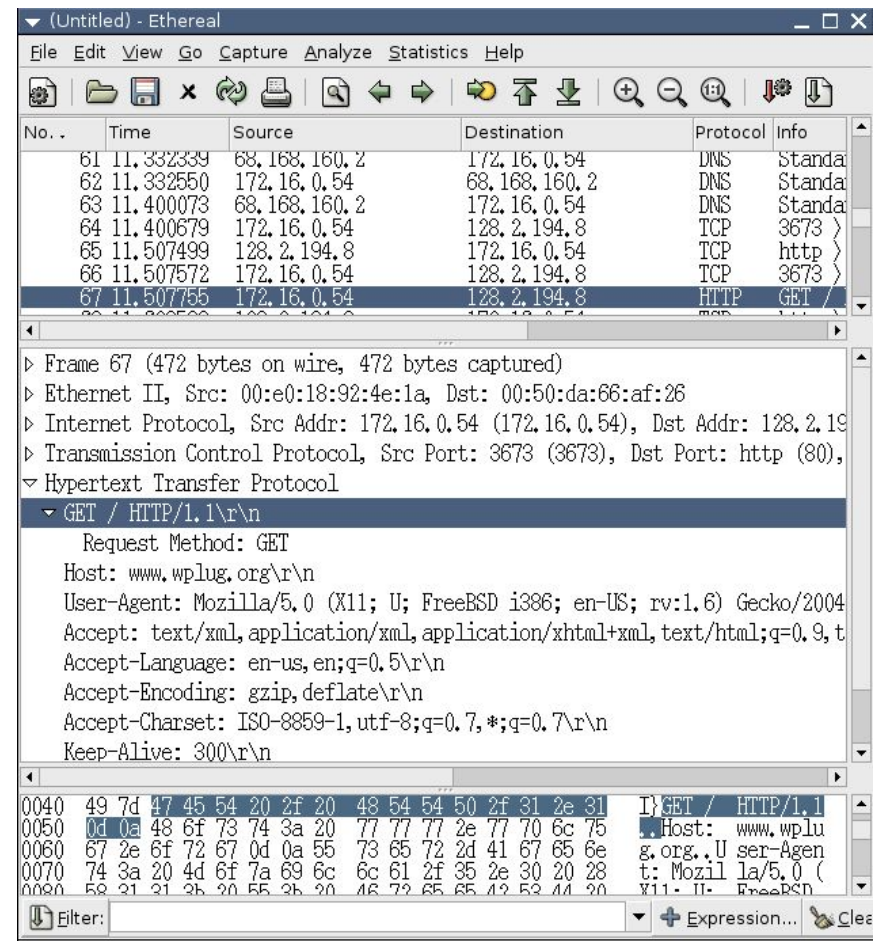
Monitoring: seeing what's happening

Tcpdump:

- Comes installed with most Posix systems (Linux, BSD, etc).
- Not very easy to use.

Ethereal:

- Not usually installed by default.
- Nice GUI that dissects network traffic to help you understand it.
- Available for Windows.



snort: automated monitoring and reaction

- snort can be run as a basic packet sniffer (just like tcpdump)
- snort can also be programmed to take certain actions when certain traffic is observed (i.e. Email the administrator if a single IP address causes multiple HTTP 404 errors – see next example)
- Excellent usage: A dedicated computer that only runs snort (and is thus invisible to attackers) but can monitor all traffic to servers.
- Home usage: run snort on your home computer to be alerted when someone is trying to do something nasty.

An example attack (HTTP)

```
[02/Apr/2004:21:31:13 -0500] "GET /scripts/root.exe?/c+dir HTTP/1.0" 404 288 "-" "-"
[02/Apr/2004:21:31:14 -0500] "GET /MSADC/root.exe?/c+dir HTTP/1.0" 404 286 "-" "-"
[02/Apr/2004:21:31:17 -0500] "GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 296 "-" "-"
[02/Apr/2004:21:31:17 -0500] "GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 296 "-" "-"
[02/Apr/2004:21:31:17 -0500] "GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 310 "-" "-"
[02/Apr/2004:21:31:18 -0500] "GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 327 "-"
"-
[02/Apr/2004:21:31:18 -0500] "GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 327 "-"
"-
[02/Apr/2004:21:31:21 -0500] "GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%
1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 343 "-" "-"
[02/Apr/2004:21:31:21 -0500] "GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 309 "-" "-"
[02/Apr/2004:21:31:25 -0500] "GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 309 "-" "-"
[02/Apr/2004:21:31:25 -0500] "GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 309 "-" "-"
[02/Apr/2004:21:31:25 -0500] "GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 309 "-" "-"
[02/Apr/2004:21:31:25 -0500] "GET /scripts/..%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 400 293 "-" "-"
[02/Apr/2004:21:31:26 -0500] "GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 400 293 "-" "-"
[02/Apr/2004:21:31:26 -0500] "GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 310 "-" "-"
[02/Apr/2004:21:31:26 -0500] "GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 310 "-" "-"
```

What did I do?

- whois lookup on the IP, send a copy of the log entries to the abuse address for the ISP.
- Blocked that IP using my packet filter for the next month.
- How can I automatically detect this in the future?

Example: Attempt to hijack an SMTP server

```
Feb  2 12:53:40 internet saslauthd[12524]: do_auth          : auth failure:  
[user=webmaster] [service=smtp] [realm=] [mech=pam] [reason=PAM auth error]  
  
Feb  2 12:53:44 internet saslauthd[12525]: do_auth          : auth failure:  
[user=webmaster] [service=smtp] [realm=] [mech=pam] [reason=PAM auth error]  
  
Feb  2 12:53:48 internet saslauthd[12526]: do_auth          : auth failure:  
[user=webmaster] [service=smtp] [realm=] [mech=pam] [reason=PAM auth error]  
  
Feb  2 12:53:56 internet saslauthd[12527]: do_request       : NULL password received
```

What do I do?

- Correlate these log entries with the maillog entries to get an IP. whois lookup on the IP, send a copy of the log entries to the abuse address for the ISP.
- Blocked that IP using my packet filter for the next month.
- How can I automatically detect this in the future?

Example: DDoS attack

- Immediately block the worst offenders at border firewalls if possible.
- Depending on company policy, it may be worthwhile to block entire class C blocks until the problem starts to mitigate
- Contact ISPs responsible. You'll probably need to make phone calls.
- You may get some relief by temporarily lowering the timeout on the service being attacked. (Most DoS attacks overload the number of connections available, not the bandwidth)
- Cancel your golf outings for the afternoon, you'll be busy.

References

- <http://www.newsforge.com/software/04/02/28/013>
- This file is available at
<http://www.potentialtech.com/wmoran/>