

TCPDUMP

#01

TCPDUMP

TCPDUMP ?

)
TCP/IP

Wireshark

가

가

(**Basic / Expression / Header Flag**)

Basic ()

-i : 가
-c :
-v : -vv
-n : IP . -nn Port
-w : .pcap . -r TXT

(-i) 100 (-c) .pcap
(-w) txt 가 Binary -r wireshark

```
tcpdump -i ens33 -vv -c 100 -w ttt.pcap
tcpdump: listening on ens33, link-type EN10MB (Ethernet),
capture size 262144 bytes
100 packets captured
100 packets received by filter
```

0 packets dropped by kernel

```
#          (-i)          5  (-c) DNS/PORT          IP
          (-nn)          .
tcpdump -i br0 -n -c 5
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on br0, link-type EN10MB (Ethernet), capture size
262144 bytes
14:08:14.531606 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:15.533556 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:16.535615 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:18.531679 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:19.533632 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

```
#          ( -v , -vv )          .
tcpdump -i br0 -n -vv -c 5
tcpdump: listening on br0, link-type EN10MB (Ethernet),
capture size 262144 bytes
14:10:46.548613 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:47.549640 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:48.551557 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:50.548614 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:51.549621 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

(-i) IP 가 (-nn, grep)

tcpdump -i ens33 -nn | grep "1.2.3.4"

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes

5 packets captured

6 packets received by filter

0 packets dropped by kernel

14:28:31.524052 IP 1.2.3.4.22 > 5.6.7.8.53707: Flags [P.], seq 4138122029:4138122237, ack 1068364849, win 1432, length 208

14:28:31.525940 IP 5.6.7.8.53707 > 1.2.3.4.22: Flags [.], ack 208, win 509, length 0

Expression ()

. 가 .

1) Type ()

- host , net , port

2) Dir ()

- src, dst , src or dst, src and dst

3) Proto ()

- ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp, udp

4)

- ('and(&&)', 'or(||)', 'not(!)')

- gateway, broadcast, less, greater

(-i) tcp Destination Port 가 22

IP (-nn)

tcpdump -i ens33 tcp dst port 22 -nn

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes

16:50:25.964928 IP 211.115.223.215.53707 > 211.239.150.48.22: Flags [.], ack 4194846013, win 511, length 0

```
16:50:26.016014 IP 211.115.223.215.53707 > 211.239.150.48.22:
Flags [.], ack 161, win 511, length 0
16:50:26.060903 IP 211.115.223.215.53707 > 211.239.150.48.22:
Flags [.], ack 321, win 510, length 0
```

```
# (-i) tcp " Destination Port 가 80 "
" 443 IP (-nn)
```

```
tcpdump -i ens33 -nn tcp and dst port 80 or dst port 443
```

```
16:59:12.840778 IP 211.239.150.48.49514 > 8.8.8.8.443: Flags
[F.], seq 5, ack 9, win 229, options [nop,nop,TS val
3924566459 ecr 3515313672], length 0
16:59:14.863982 IP 211.239.150.48.47286 > 8.8.8.8.80: Flags
[S], seq 873533324, win 29200, options [mss 1460,sackOK,TS val
3924568482 ecr 0,nop,wscale 7], length 0
16:59:15.865581 IP 211.239.150.48.47286 > 8.8.8.8.80: Flags
[S], seq 873533324, win 29200, options [mss 1460,sackOK,TS val
3924569484 ecr 0,nop,wscale 7], length 0
```

Header Flag

```
#
[ ] SYN : Client 가 Server ( ) 가
IN/OUT Port
```

-
-
-

```
# SYN
= TCP Flag( tcp[13] ) SYN ( 0x02 ) IP ( -nn ) 10
(-c) txt result.log ( > )
```

```
tcpdump -i ens33 -c 10 "tcp[13] == 0x02" -n -nn > result.log
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size
262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

cat resule.log

```
16:16:15.308872 IP 211.239.150.48.43192 > 61.100.13.230.10051:
Flags [S], seq 3596242163, win 29200, options [mss
1460,sackOK,TS val 3921988927 ecr 0,nop,wscale 7], length 0
16:16:17.048128 IP 121.40.192.14.41265 > 211.239.150.48.4244:
Flags [S], seq 3887030721, win 1024, length 0
```

[S] = SYN Flag

```
json      ,      .
```

Unskilled Attackers Pester Real Security Folks

=====

TCPDUMP FLAGS

Unskilled = URG = (Not Displayed in Flag Field, Displayed elsewhere)

Attackers = ACK = (Not Displayed in Flag Field, Displayed elsewhere)

Pester = PSH = [P] (Push Data)

Real = RST = [R] (Reset Connection)

Security = SYN = [S] (Start Connection)

Folks = FIN = [F] (Finish Connection)

SYN-ACK = [S.] (SynAck Packet)

[.] (No Flag Set)

JSON

result.log

IP: 211.239.150.48

JSON:

```
[ { ipaddr1: '221.239.150.48',
  ipaddr2: '61.100.13.230',
  type: 'Outbound',
  port: '10051' },
  { ipaddr1: '121.40.192.14',
  ipaddr2: '221.239.150.48',
  type: 'Inbound',
  port: '4244' } ]
```

Table:

ipaddr1	ipaddr2	type	port
---------	---------	------	------

221.239.150.48 61.100.13.230 Outbound 10051
121.40.192.14 211.239.150.48 Inbound 4244

TCP 3 way handshark : <https://websecurity.tistory.com/93>

Surge

Surge

CDN surge
CDN
/ 가 ,
가 1 30[\$] 가

Surge

- custom domain 가 .
- Web Cache , Client Cache-Control
가 . (ETag)
- Gzip .

Surge

- . (가 , .)
- http2

Surge

NodeJS

nvm

NodeJS

```
curl https://raw.githubusercontent.com/nvm-sh/nvm/v0.39.1/install.sh | bash -o -  
. ~/.bashrc  
nvm install --lts  
nvm ls
```

```
node --version
```

```
npm install --global surge
```

Surge

Surge 1

```
mkdir test && cd test/
```

```
echo hello > index.html
```

```
surge
```

```
project: /home/user/test/
```

```
## CDN
```

```
domain: noiseless-duck.surge.sh
```

```
##
```

```
## Aborted 가
```

```
## Success!
```

```
가
```

```
curl -I https://noiseless-duck.surge.sh
```

```
## HTTP/1.1 200 OK
```

Surge 2

surge

```
mkdir test && cd test/
```

```
echo "index" > index.html
```

```
mkdir ignore/
```

```
echo "ignore/index" > ignore/index.html
```

```
.surgeignore 200.html
```

```
# .surgeignore
```

```
echo "ignore/" > .surgeignore
```

```
#
```

```
## .git
```

```
## .*
```

```
## *.*~
```

```
## node_modules
```

```
## bower_components
```

```
# 200.html
```

```
## 404 가 200.html
```

```
echo "200" > 200.html
```

```
surge ./ --domain noiseless-duck.surge.sh
```

```
## ./ noiseless-duck.surge.sh
```

```
curl https://noiseless-duck.surge.sh
```

```
## index.html
```

```
curl https://noiseless-duck.surge.sh/notexist
```

```
## 404 -> 200.html
```

```
curl https://noiseless-duck.surge.sh/ignore
```

```
## .surgeignore -> 404 -> 200.html
```



```
surge list
```

```
##
```

```
surge teardown noiseless-duck.surge.sh
```

```
##
```

```
surge logout
```

```
##
```

Surge

surge

가

surge

<https://surge.sh/help/>

Amazon Elastic Container Registry Public (ECR Public)

Amazon Elastic Container Registry Public (ECR Public)

[Amazon Elastic Container Registry Public \(ECR Public\)](#)

—

—

[Service Quotas](#)

[Amazon ECR Public Gallery](#)

가

[Push](#)

[pull](#)

Amazon Elastic Container Registry(Amazon ECR) 가
AWS
Amazon ECR AWS IAM /
AWS ECS, EKS ECR .

<https://aws.amazon.com/ko/ecr/pricing/>



- Docker Hub
 - <https://www.docker.com/pricing/>

Service Quotas

<https://us-west-1.console.aws.amazon.com/servicequotas/home/services/ecr/quotas>
s



Amazon ECR Public Gallery

<https://gallery.ecr.aws/>

Amazon ECR

Amazon ECR



가



- *AWS CLI*

- https://docs.aws.amazon.com/ko_kr/cli/v1/userguide/cli-chap-install.html

-





Push



ecr-public endpoints

- AWS CLI AWS SDK



-

Docker

```
root@hostway-bmt:~# aws ecr-public get-login-password --  
region us-east-1 | docker login --username AWS --  
password-stdin public.ecr.aws/n3n4q5v6
```

WARNING! Your password will be stored unencrypted in
/root/.docker/config.json. Configure a credential helper
to remove this warning. See

<https://docs.docker.com/engine/reference/commandline/login/#credentials-store>

Login Succeeded

-

```
root@hostway-bmt:~# docker tag grafana:8.0.4  
public.ecr.aws/n3n4q5v6/ecr-bmt-hostway:8.0.4
```

```
root@hostway-bmt:~# docker images
```

REPOSITORY	TAG	IMAGE
------------	-----	-------

ID	CREATED	SIZE	
grafana			8.0.4
4a61138b1602	2 weeks ago	206MB	
public.ecr.aws/n3n4q5v6/ecr-bmt-hostway			8.0.4
4a61138b1602	2 weeks ago	206MB	

▪ AWS

```

root@hostway-bmt:~# docker push
public.ecr.aws/n3n4q5v6/ecr-bmt-hostway:8.0.4
The push refers to repository
[public.ecr.aws/n3n4q5v6/ecr-bmt-hostway]
53fb6eb29c9d: Pushed
1fc7a3b8385e: Pushed
271c2e7e76f9: Pushed
5f70bf18a086: Pushed
9f9cedf089aa: Pushing [=====>
                    ] 103.6MB/182.1MB
3c960bff45aa: Pushed
efd53ffe2857: Pushing
[=====>]
5.707MB
30a972c8cd3c: Pushed
b2d5eeeaba3a: Pushing
[=====>]
5.88MB
8.0.4: digest:
sha256:fa1f0fef19321a5p1apcee215febe02ad3fb1a992a4d5e369
b7f651b3epeb13f size: 2199

```



pull

```
root@hostway-bmt:~# docker pull public.ecr.aws/n3n4q5v6/ecr-  
bmt-hostway:8.0.4  
8.0.4: Pulling from n3n4q5v6/ecr-bmt-hostway  
Digest:  
sha256:fa1f0fef19321a5p1apcee215febe02ad3fb1a992a4d5e369b7f651  
b3ebeb13f  
Status:          Downloaded newer image for  
public.ecr.aws/n3n4q5v6/ecr-bmt-hostway:8.0.4  
public.ecr.aws/n3n4q5v6/ecr-bmt-hostway:8.0.4
```

[Windows] []

CredSSP

Oracle

Windows Server

가

CredSSP

[Window Title]

[Content]

가 .
가 .

CredSSP :
<https://go.microsoft.com/fwlink/?linkid=866660>



CredSSP 1

Client PC

Wins + R "gpedit.msc"



-> -> -> -> Oracle



- : " "



+ R => "cmd"



gpupdate /force



CredSSP 2

Client: PC Windows Update
Server: Windows Update

[Container Runtime] CRI-O

가

CRI-O 가

CRI-O ?

CRI-O OCI (CRI) .
가 Docker Kubernetes 1.24
Docker CRI() shim
(Docker Engine) CRI-O 가 .

(VM)

Controller Server : 1EA

Worker Server : 1EA

OS

Ubuntu 20.04 Server Minimal

<https://github.com/cri-o/cri-o/blob/main/install.md#supported-versions> :

: <https://tech.hostway.co.kr/2022/02/06/418/>

Traffic Setup

```
# .conf
```

```
# Controller / Worker
```

```
cat <<EOF | sudo tee /etc/modules-load.d/crio.conf  
overlay  
br_netfilter  
EOF
```

```
sudo modprobe overlay
```



```
sudo modprobe br_netfilter
```

```
# sysctl , .
```

```
# Controller / Worker
```

```
cat <<EOF | sudo tee /etc/sysctl.d/99-kubernetes-cri.conf
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 1
EOF
```

```
sudo sysctl --system
```

cgroup driver

```
# CRI-O systemd cgroup .
```

```
cgroupfs cgroup , /etc/crio/crio.conf
/etc/crio/crio.conf.d/02-cgroup-manager.conf -
(drop-in) .
```

```
[crio.runtime]
common_cgroup = "pod"
cgroup_manager = "cgroupfs"
```

CRI-O

```
# Controller / Worker
```

```
sudo -i
export OS=xUbuntu_20.04 # OS
export VERSION=1.19 # cri-o
```

```
echo "deb
https://download.opensuse.org/repositories/devel:/kubic:/libco
ntainers:/stable/$OS/ /" >
/etc/apt/sources.list.d/devel:kubic:libcontainers:stable.list
echo "deb
http://download.opensuse.org/repositories/devel:/kubic:/libcon
```

```
tainers:/stable:/cri-o:/$VERSION/$OS/      /"      >
/etc/apt/sources.list.d/devel:kubic:libcontainers:stable:cri-
o:$VERSION.list
```

```
curl -L
https://download.opensuse.org/repositories/devel:kubic:libcont
ainers:stable:cri-o:$VERSION/$OS/Release.key | apt-key add -
curl -L
https://download.opensuse.org/repositories/devel:/kubic:/libco
ntainers:/stable/$OS/Release.key | apt-key add -
```

```
sudo apt-get update
```

```
sudo apt-get install cri-o cri-o-runc
```

```
sudo systemctl daemon-reload
sudo systemctl enable crio --now
sudo systemctl status crio
```

Controller Node Initialize

```
# docker 1 CRI-
0
```

```
# Controller
```

```
kubeadm init --cri-socket=/var/run/crio/crio.sock --ignore-
preflight-errors=all --pod-network-cidr=192.168.0.0/16 --
apiserver-advertise-address=203.248.23.192
```

```
# Worker
```

```
kubeadm join 203.248.23.192:6443 --token
9oy7rn.qtw04nfd8ga417p4 --discovery-token-ca-cert-hash
sha256:26218e0c80320b7c23735916c130fc48f644b26314212d917969553
ec0651256
```

Outlook 2016 PST

가

Outlook PST

1. Outlook -> .



2. 가 / .



3. - (N) .



4. Outlook (.pst) (N) .



5. (N) .

((S) ,
가 .)



6. .



7. .



8. .



Outlook PST

1. Outlook ->



2. 가 /



3. 가 -

(N)



4. Outlook (.pst)

(N)



5. (.pst)

(N)



6. 가



7.



8. Outlook



Outlook 2016

Outlook

[Windows] Windows SMB

&

[Windows] Windows

& SMB

SMB

SMB

OS

MS SMB
가

SMB

가

SMB

Powershell ISE

updated by Hostway System Team

```
$Language = Get-WinUserLanguageList  
$Lang = $Language.LanguageTag
```

```
Switch($Lang)
```

```
{  
'ko'
```

```
{
```

```
Write 'OS Version'
```

```
[Environment]::OSVersion
```

```
Write-Verbose -Message "  
139, TCP 445" -Verbose
```

UDP 137, UDP 138, TCP

```
netsh advfirewall firewall set rule name="
```

(NB-Name-

```
In)" profile=public dir=in localport=137 protocol=udp new
enable=no
netsh advfirewall firewall set rule name=" (NB-Name-
In)" profile=private dir=in localport=137 protocol=udp new
enable=no
netsh advfirewall firewall set rule name=" (NB-Name-
In)" profile=public,domain dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name=" (NB-Name-
In)" profile=private,domain dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name=" (NB-Name-
In)" profile=private,public dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name=" (NB-Name-
In)" profile=any dir=in localport=137 protocol=udp new
enable=no

netsh advfirewall firewall set rule name=" (NB-
Name-In)" profile=public dir=in localport=137 protocol=udp new
enable=no
netsh advfirewall firewall set rule name=" (NB-
Name-In)" profile=private dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name=" (NB-
Name-In)" profile=public,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Name-In)" profile=private,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Name-In)" profile=private,public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Name-In)" profile=any dir=in localport=137 protocol=udp new
enable=no

netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=public dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name=" (NB-
```

```
Datagram-In)" profile=private dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=public, domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=private, domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=private, public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=any dir=in localport=137 protocol=udp
new enable=no
```

```
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=public dir=in localport=138 protocol=udp
new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=public, domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=private, domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=private, public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=any dir=in localport=138 protocol=udp
new enable=no
```

```
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=public dir=in localport=138 protocol=udp
new enable=no
netsh advfirewall firewall set rule name=" (NB-
Datagram-In)" profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=" (NB-
```

```
Datagram-In)" profile=public,domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="" (NB-
Datagram-In)" profile=private,domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="" (NB-
Datagram-In)" profile=private,public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="" (NB-
Datagram-In)" profile=any dir=in localport=138 protocol=udp
new enable=no
```

```
netsh advfirewall firewall set rule name="가 (NB-
Session-In)" profile=public dir=in localport=139 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name="가 (NB-
Session-In)" profile=private dir=in localport=139 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name="가 (NB-
Session-In)" profile=public,domain dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="가 (NB-
Session-In)" profile=private,domain dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="가 (NB-
Session-In)" profile=private,public dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="가 (NB-
Session-In)" profile=any dir=in localport=139 protocol=tcp new
enable=no
```

```
netsh advfirewall firewall set rule name="" (NB-
Session-In)" profile=public dir=in localport=139 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name="" (NB-
Session-In)" profile=private dir=in localport=139 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name="" (NB-
Session-In)" profile=public,domain dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="" (NB-
```



```
Session-In)" profile=private,domain dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Session-In)" profile=private,public dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name=" (NB-
Session-In)" profile=any dir=in localport=139 protocol=tcp new
enable=no

netsh advfirewall firewall set rule name=" (SMB-
In)" profile=public dir=in localport=445 protocol=tcp new
enable=no
netsh advfirewall firewall set rule name=" (SMB-
In)" profile=private dir=in localport=445 protocol=tcp new
enable=no
netsh advfirewall firewall set rule name=" (SMB-
In)" profile=public,domain dir=in localport=445 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name=" (SMB-
In)" profile=private,domain dir=in localport=445 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name=" (SMB-
In)" profile=private,public dir=in localport=445 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name=" (SMB-
In)" profile=any dir=in localport=445 protocol=tcp new
enable=no
}
'en-US'
{
Write 'OS Version'
[Environment]::OSVersion
Write-Verbose -Message "Vulnerability Port Removal UDP 137,
UDP 138, TCP 139, TCP 445" -Verbose

netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=public dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=private dir=in localport=137
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=public,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=private,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=private,public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=any dir=in localport=137 protocol=udp
new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=private dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=public,domain dir=in
localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=private,domain dir=in
localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=private,public dir=in
localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=any dir=in localport=137
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=public,domain dir=in localport=137
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private, domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private, public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=any dir=in localport=137
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=public, domain dir=in
localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=private, domain dir=in
localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=private, public dir=in
localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=any dir=in localport=138
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=public, domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private, domain dir=in localport=138
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery (NB-Datagram-In)" profile=private,public dir=in localport=138 protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery (NB-Datagram-In)" profile=any dir=in localport=138 protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine Monitoring (NB-Session-In)" profile=public dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine Monitoring (NB-Session-In)" profile=private dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine Monitoring (NB-Session-In)" profile=public,domain dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine Monitoring (NB-Session-In)" profile=private,domain dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine Monitoring (NB-Session-In)" profile=private,public dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine Monitoring (NB-Session-In)" profile=any dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer Sharing (NB-Session-In)" profile=public dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer Sharing (NB-Session-In)" profile=private dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer Sharing (NB-Session-In)" profile=public,domain dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer Sharing (NB-Session-In)" profile=private,domain dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer Sharing (NB-Session-In)" profile=private,public dir=in localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Session-In)" profile=any dir=in localport=139
protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote
Management (SMB-In)" profile=public dir=in localport=445
protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote
Management (SMB-In)" profile=private dir=in localport=445
protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote
Management (SMB-In)" profile=public,domain dir=in
localport=445 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote
Management (SMB-In)" profile=private,domain dir=in
localport=445 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote
Management (SMB-In)" profile=private,public dir=in
localport=445 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote
Management (SMB-In)" profile=any dir=in localport=445
protocol=tcp new enable=no
```

```
}
```

```
}
```