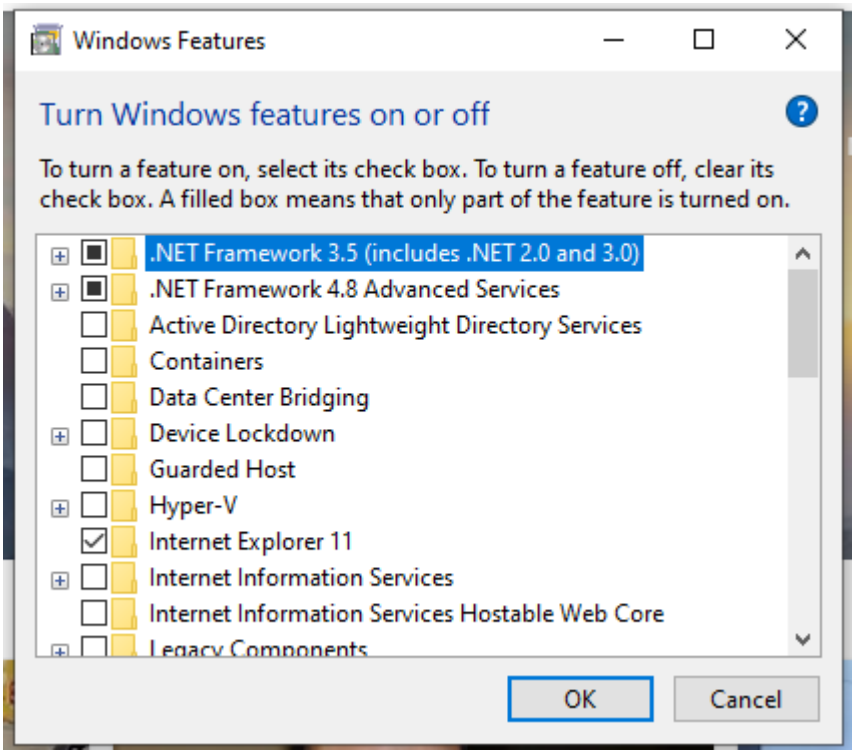
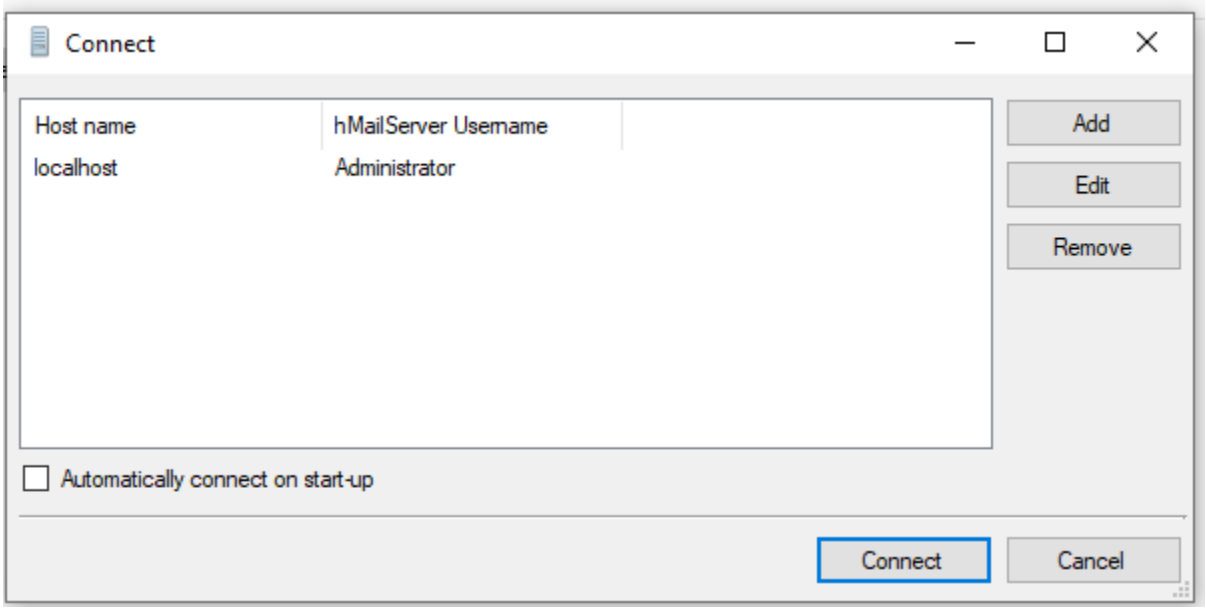
Kịch bản honeypot ở localnet: kịch bản này ta sẽ xây dựng một mail server đơn giản ở Windows để nhận alert từ honeypot `Kfsensor`, bao gồm mail server,client lần lượt là hmailserver, thunderbird.

1. Cài đặt

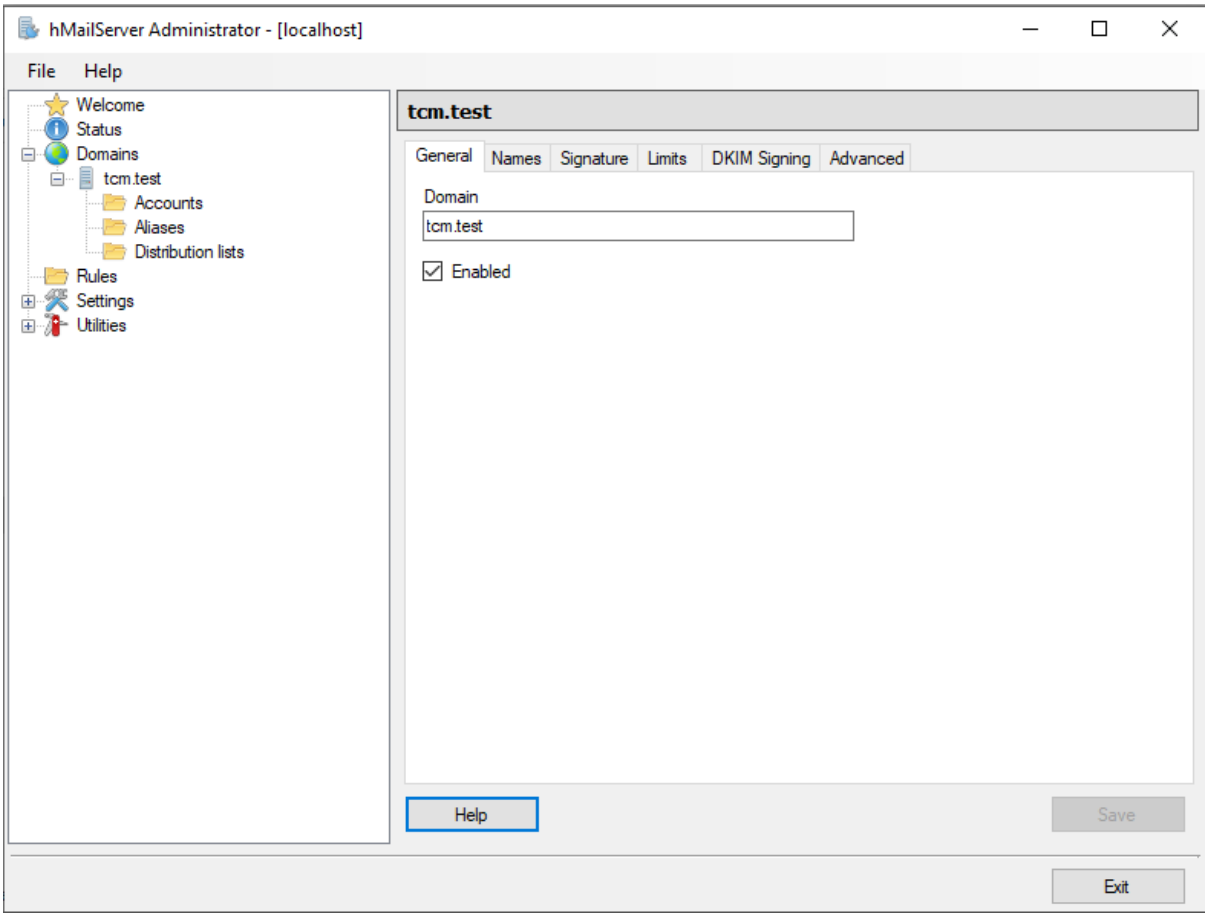
- Enable feature .NET 3.5 của Windows (mặc định sẽ tắt) dùng để cài đặt `hmailserver`.



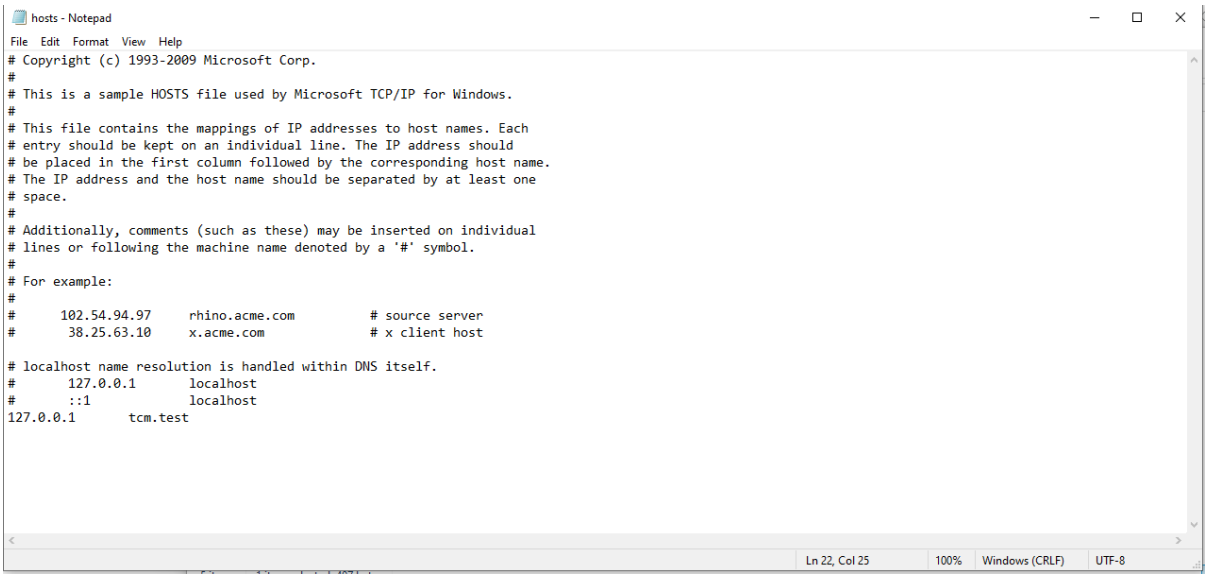
- Cài đặt hmailserver
    - Giao diện kết nối của `hmailserver` sau khi cài đặt



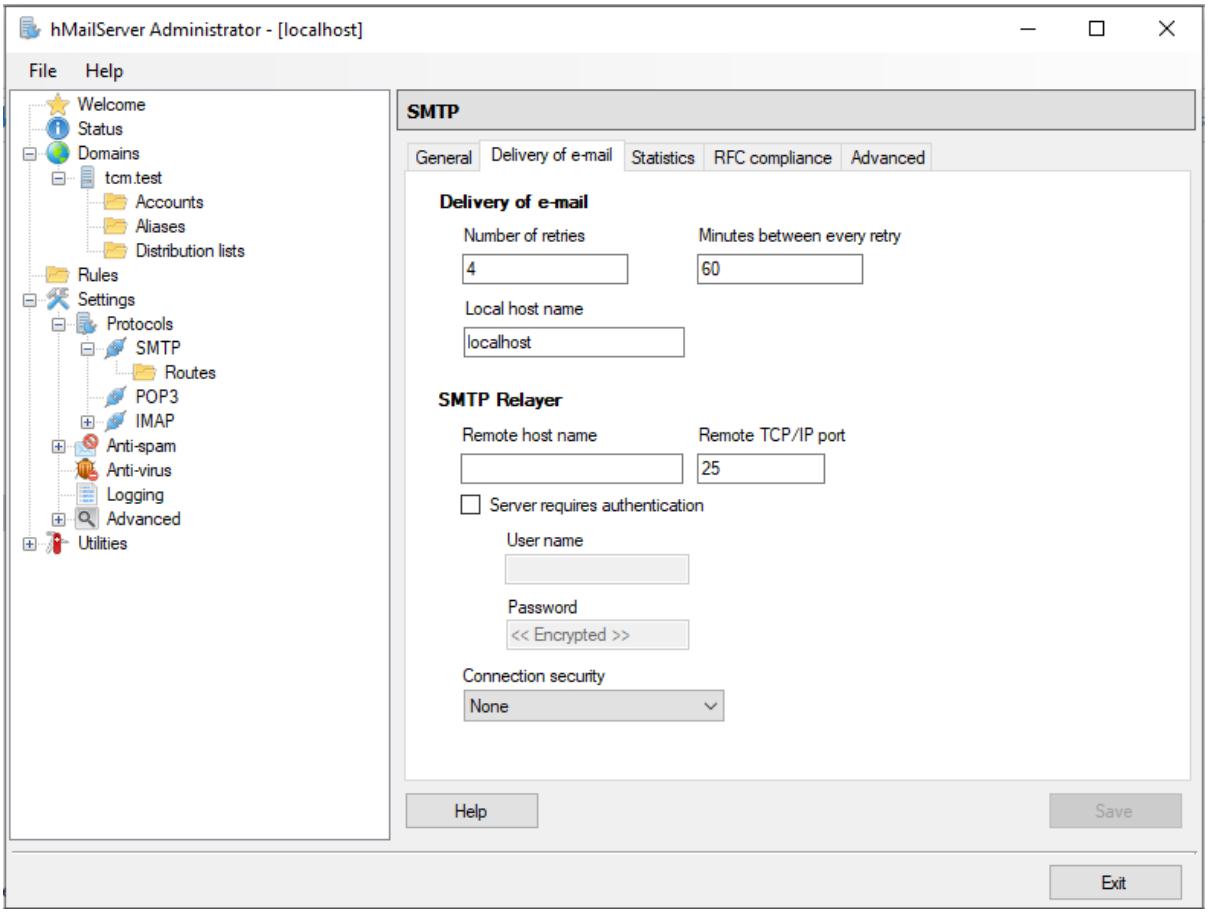
- Tạo domain `tcm.test`



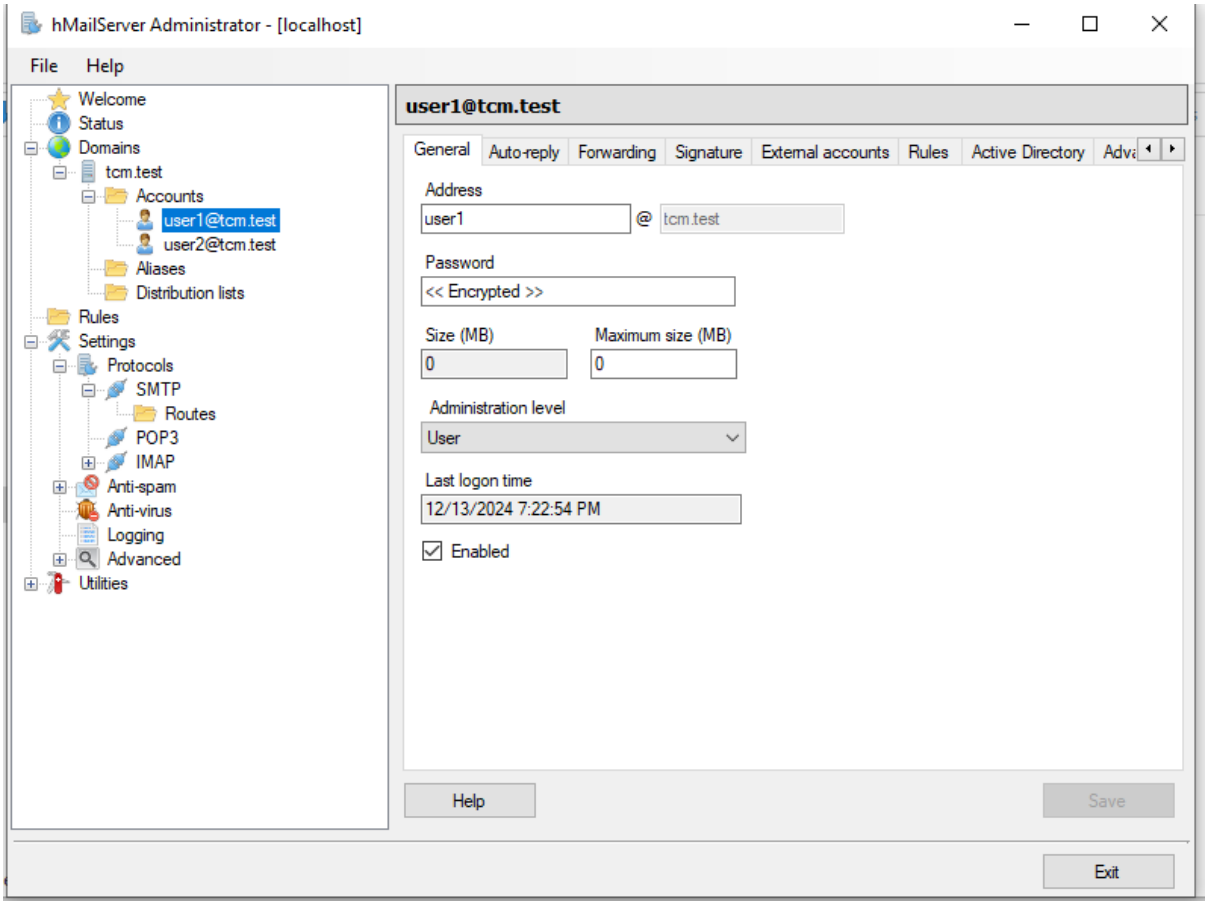
- Thêm domain vào file host của Windows



- Thêm hostname vào phần SMTP

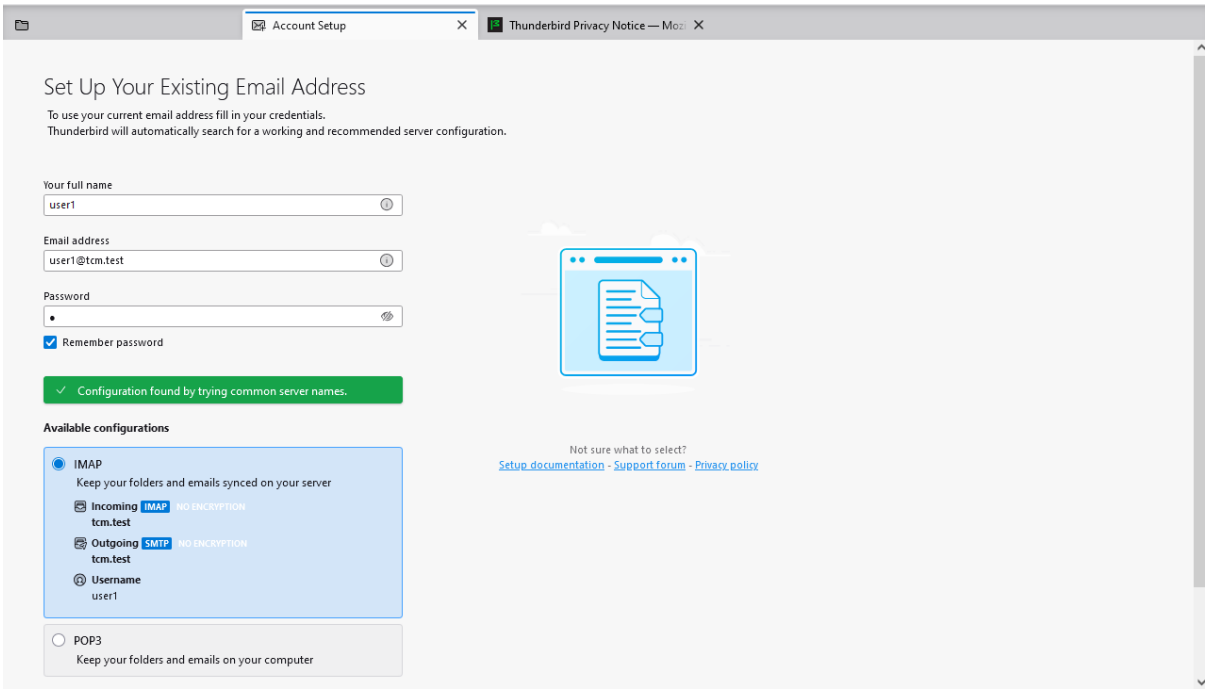


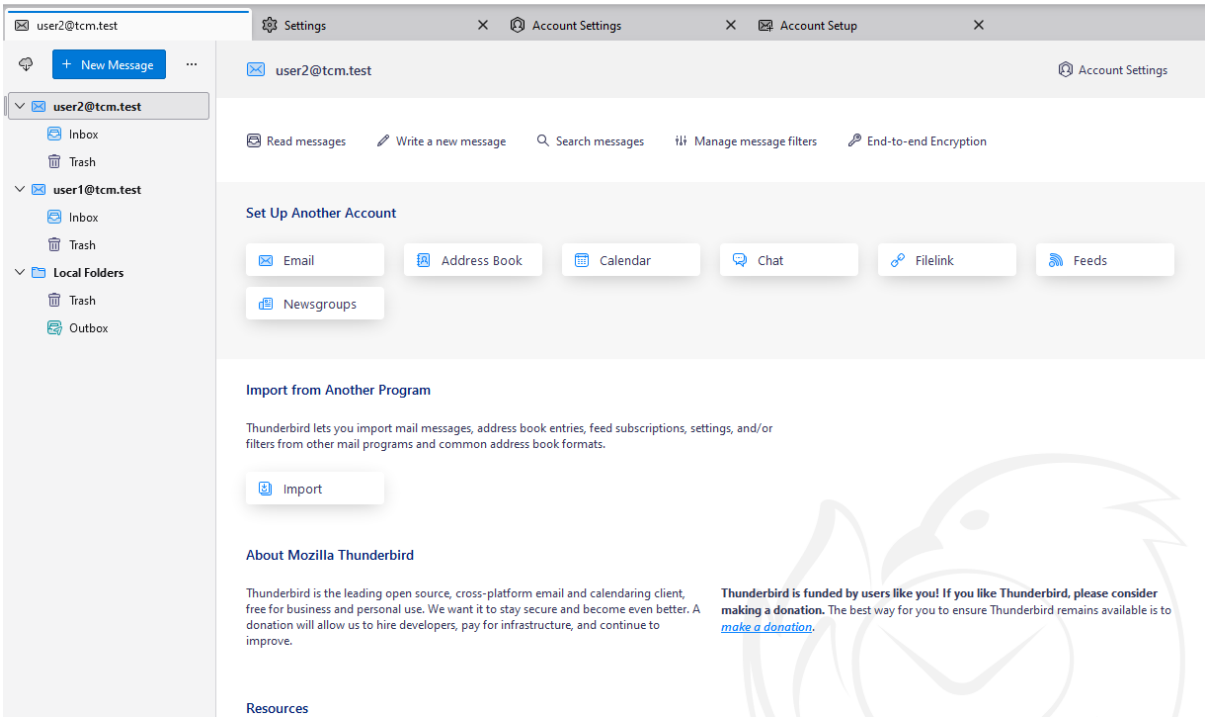
- Tạo 2 account để test



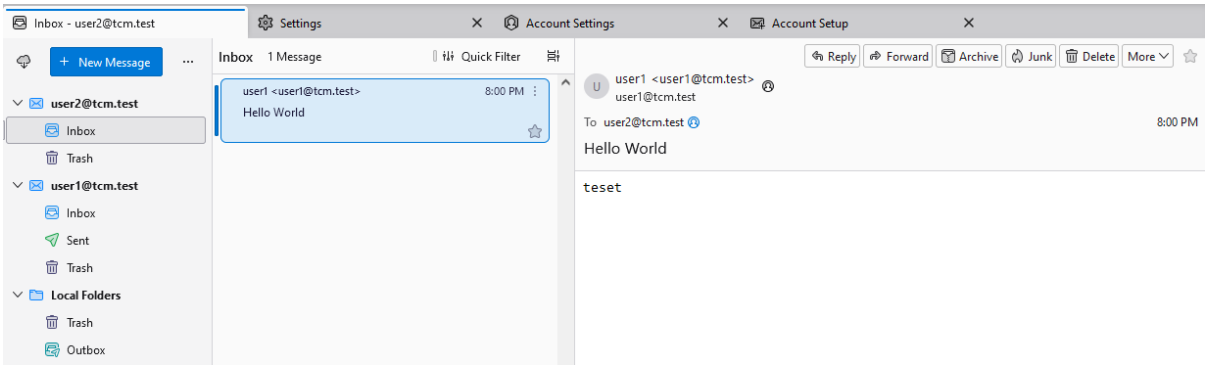
- Cài đặt thunderbird

- Thêm account vào thunderbird



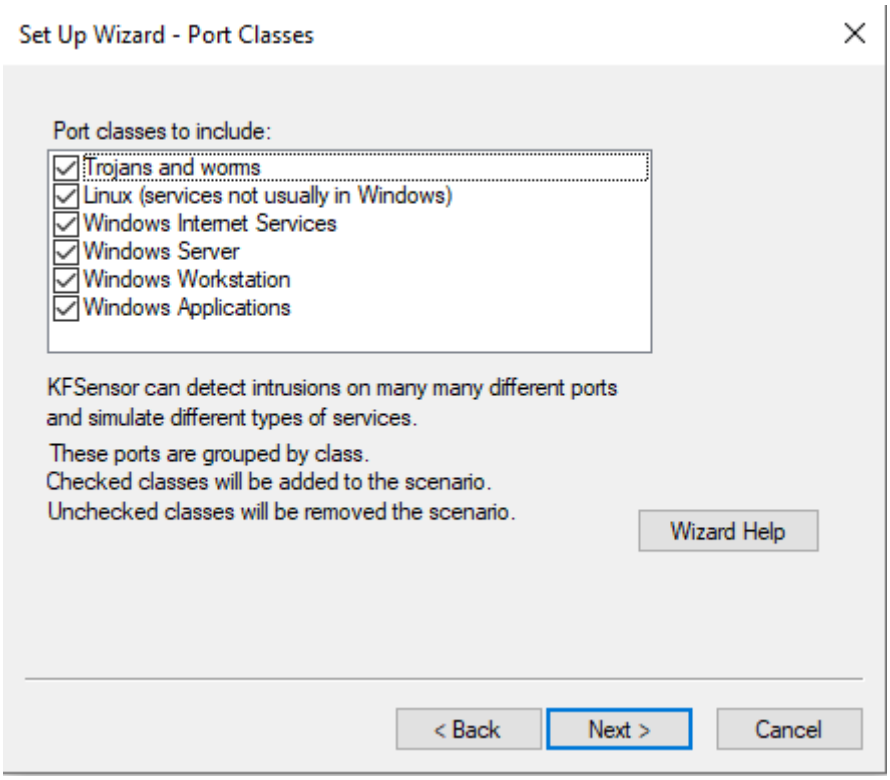


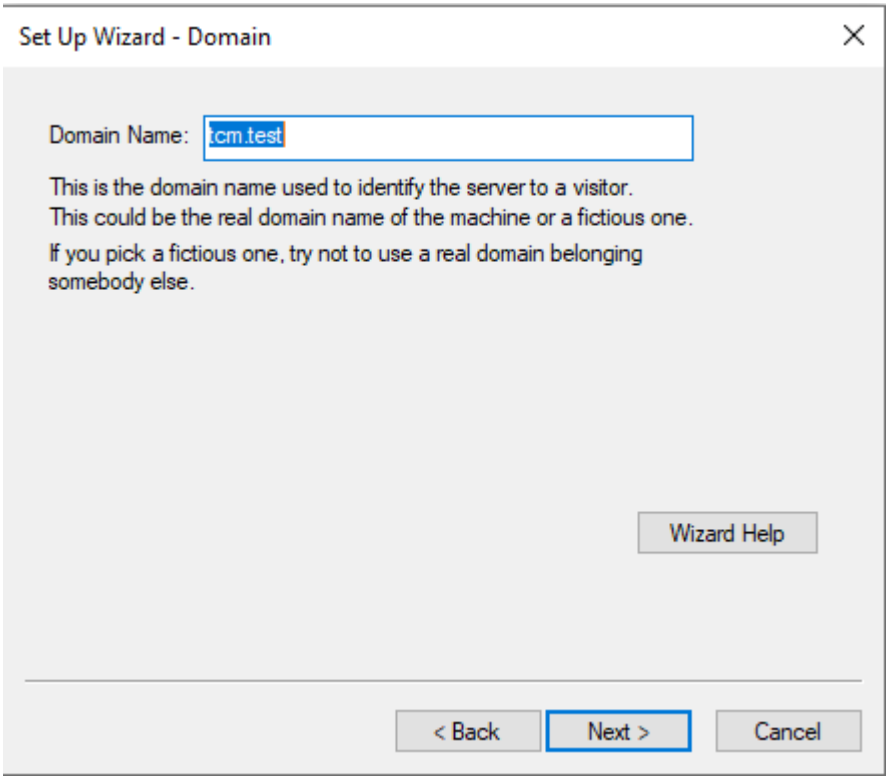
- Kiểm tra kết nối

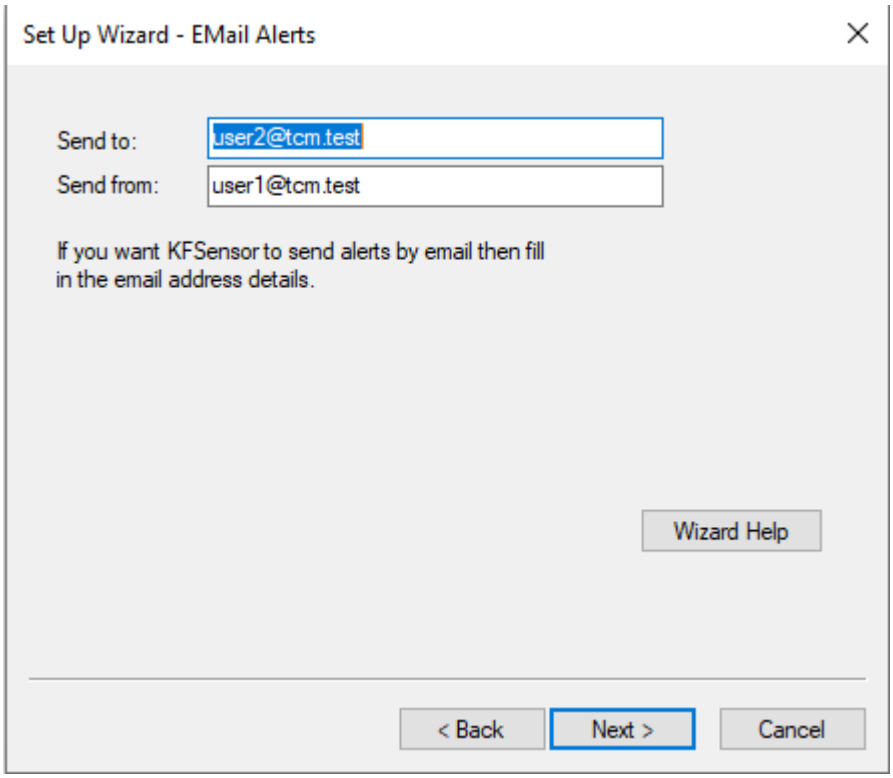


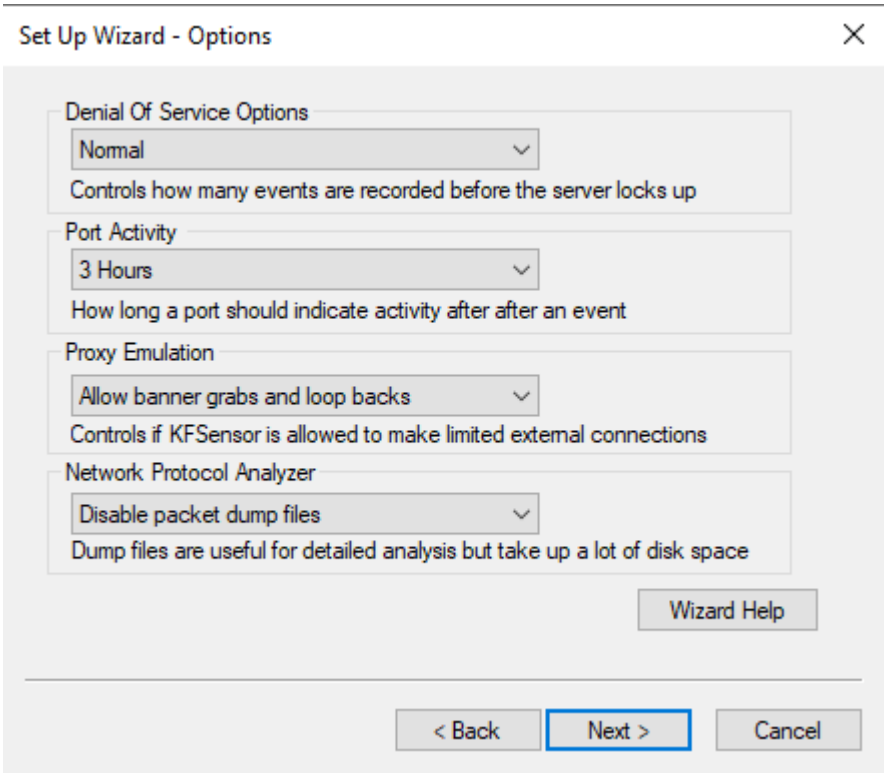
- Cài đặt Kfsensor Cài đặt npcap tại https://nmap.org/npcap/dist/npcap-1.77.exe

- Cấu hình kfsensor



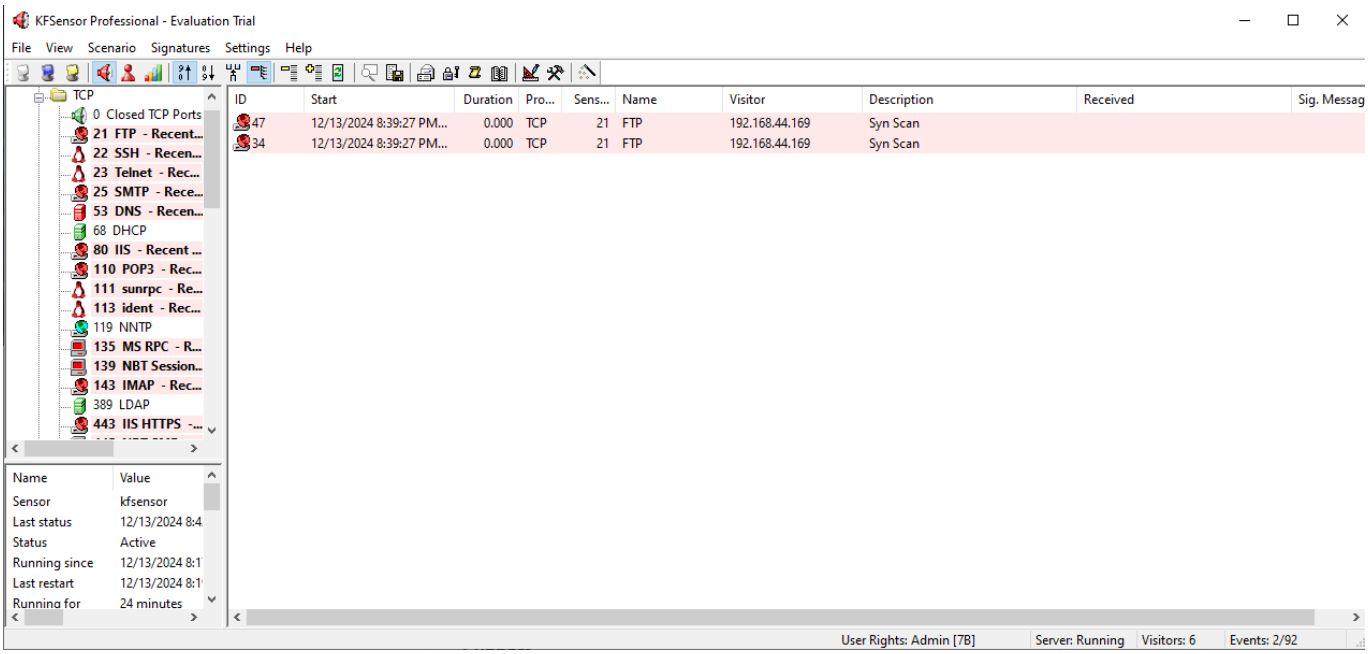






Kịch bản tấn công

- Port scan Sau khi cài kfsensor một số port sẽ được mở trên windows cho attacker thực hiện scan, thông tin từ đây cũng sẽ bị capture lại, tuy nhiên thì sau khi scan attacker sẽ không thấy gì ngoại trừ phía honeypot

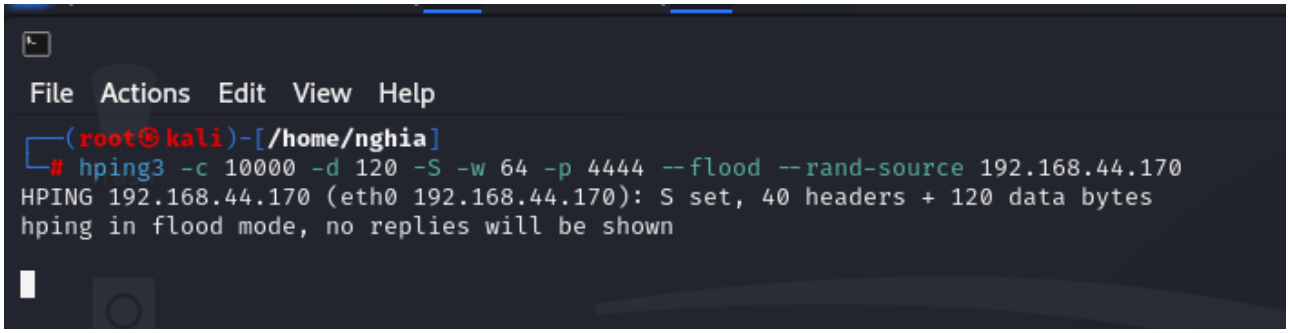


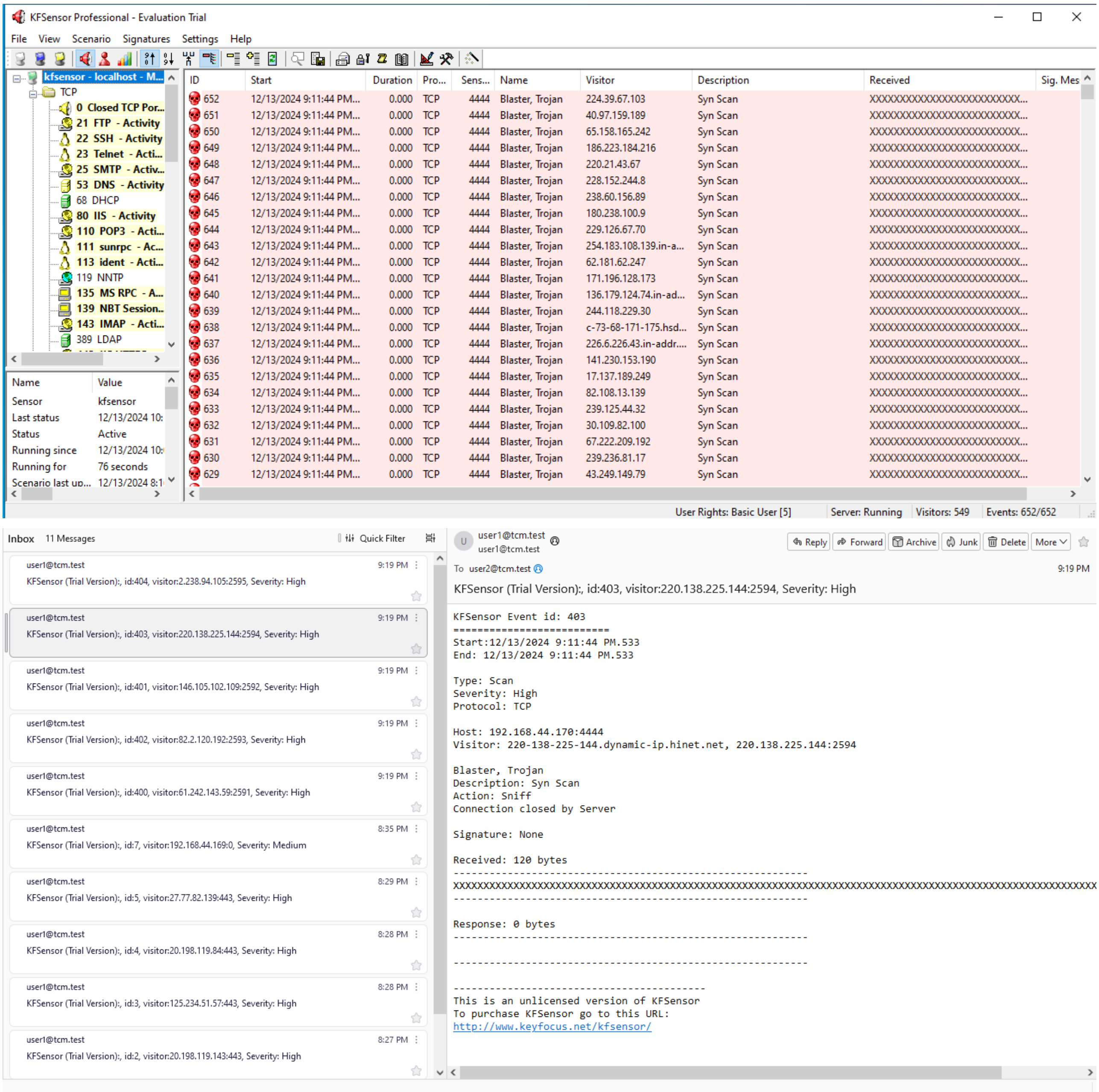

```
└─# nmap -T4 -p- -A 192.168.44.170
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 23:39 EST
Stats: 0:07:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 31.89% done; ETC: 00:01 (0:15:12 remaining)
Nmap scan report for 192.168.44.170 (192.168.44.170)
Host is up (0.0016s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
7680/tcp open  pando-pub?
MAC Address: 00:0C:29:68:DD:06 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2019 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.58 ms 192.168.44.170 (192.168.44.170)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1081.68 seconds
```

- DDOS attack




KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help
kfsensor - localhost - M...
TCP
0 Closed TCP Por...
21 FTP - Activity
22 SSH - Activity
23 Telnet - Acti...
25 SMTP - Activ...
53 DNS - Activity
68 DHCP
80 IIS - Activity
110 POP3 - Acti...
111 sunrpc - Ac...
113 ident - Acti...
119 NNTP
135 MS RPC - A...
139 NBT Session...
143 IMAP - Acti...
389 LDAP
ID Start Duration Pro... Sens... Name Visitor Description Received Sig. Mes
652 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 224.39.67.103 Syn Scan
651 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 40.97.159.189 Syn Scan
650 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 65.158.165.242 Syn Scan
649 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 186.223.184.216 Syn Scan
648 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 220.21.43.67 Syn Scan
647 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 228.152.244.8 Syn Scan
646 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 238.60.156.89 Syn Scan
645 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 180.238.100.9 Syn Scan
644 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 229.126.67.70 Syn Scan
643 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 254.183.108.139.in-a... Syn Scan
642 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 62.181.62.247 Syn Scan
641 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 171.196.128.173 Syn Scan
640 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 136.179.124.74.in-ad... Syn Scan
639 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 244.118.229.30 Syn Scan
638 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan c-73-68-171-175.hsd... Syn Scan
637 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 226.6.226.43.in-addr.... Syn Scan
636 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 141.230.153.190 Syn Scan
635 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 17.137.189.249 Syn Scan
634 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 82.108.13.139 Syn Scan
633 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 239.125.44.32 Syn Scan
632 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 30.109.82.100 Syn Scan
631 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 67.222.209.192 Syn Scan
630 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 239.236.81.17 Syn Scan
629 12/13/2024 9:11:44 PM... 0.000 TCP 4444 Blaster, Trojan 43.249.149.79 Syn Scan
Name Value
Sensor kfsensor
Last status 12/13/2024 10:
Status Active
Running since 12/13/2024 10:
Running for 76 seconds
Scenario last up... 12/13/2024 8:1
User Rights: Basic User [5] Server: Running Visitors: 549 Events: 652/652
Inbox 11 Messages Quick Filter
user1@tcm.test 9:19 PM
KFSensor (Trial Version):, id:404, visitor:2.238.94.105:2595, Severity: High
user1@tcm.test 9:19 PM
KFSensor (Trial Version):, id:403, visitor:220.138.225.144:2594, Severity: High
user1@tcm.test 9:19 PM
KFSensor (Trial Version):, id:401, visitor:146.105.102.109:2592, Severity: High
user1@tcm.test 9:19 PM
KFSensor (Trial Version):, id:402, visitor:82.2.120.192:2593, Severity: High
user1@tcm.test 9:19 PM
KFSensor (Trial Version):, id:400, visitor:61.242.143.59:2591, Severity: High
user1@tcm.test 8:35 PM
KFSensor (Trial Version):, id:7, visitor:192.168.44.169:0, Severity: Medium
user1@tcm.test 8:29 PM
KFSensor (Trial Version):, id:5, visitor:27.77.82.139:443, Severity: High
user1@tcm.test 8:28 PM
KFSensor (Trial Version):, id:4, visitor:20.198.119.84:443, Severity: High
user1@tcm.test 8:28 PM
KFSensor (Trial Version):, id:3, visitor:125.234.51.57:443, Severity: High
user1@tcm.test 8:27 PM
KFSensor (Trial Version):, id:2, visitor:20.198.119.143:443, Severity: High
user1@tcm.test
user1@tcm.test
Reply Forward Archive Junk Delete More
To user2@tcm.test 9:19 PM
KFSensor (Trial Version):, id:403, visitor:220.138.225.144:2594, Severity: High
KFSensor Event id: 403
=========================
Start:12/13/2024 9:11:44 PM.533
End: 12/13/2024 9:11:44 PM.533
Type: Scan
Severity: High
Protocol: TCP
Host: 192.168.44.170:4444
Visitor: 220-138-225-144.dynamic-ip.hinet.net, 220.138.225.144:2594
Blaster, Trojan
Description: Syn Scan
Action: Sniff
Connection closed by Server
Signature: None
Received: 120 bytes
Response: 0 bytes
This is an unlicensed version of KFSensor
To purchase KFSensor go to this URL:
http://www.keyfocus.net/kfsensor/