

py scripts from other repo's that i use (need to add to my repo)

https://github.com/Crypto-Cat/CTF/blob/main/pentesting/gen_nmap.py

```
#!/bin/python
#
# can be found on crypto cat's repo,
# https://github.com/Crypto-Cat/CTF/blob/main/pentesting/gen_nmap.py
#
# sudo apt-get install python3 masscan nmap
#
# This script will take in Masscan results and produce an output which can be fed into NMap

# Save your Masscan result as mscan.txt then run this script to produce nmap.txt then you can
run:
# while read item; do sudo nmap -sV -sC -sS -sU $item; done < nmap.txt; rm mscan.txt nmap.txt

# If you want to export to .xml file you can use the following command and then later use this
script to merge files: https://github.com/sidaf/scripts/blob/master/nmap_merge.py
# while read item; do filename=$(echo $item | grep -o "^\S*"); sudo nmap -O -sV -sC -sS -sU
$item -oX $filename.xml; done < nmap.txt

import re
from socket import inet_aton
from os import path

regex = re.compile(r"Discovered open port (\d+)\[(udp|tcp)\] on (\d+\.\d+\.\d+\.\d+)", re.I)

ip_list = {}

with open(path.abspath('mscan.txt')) as f:
    lines = f.readlines()
    for line in lines:
        port = regex.match(line).group(1)
        protocol = regex.match(line).group(2)
```

```

ip = regex.match(line).group(3)

# Add the IP to dictionary if it's not already
try:
    ip_list[ip]
except KeyError:
    ip_list[ip] = {}

# Add protocol to dictionary if it's not already
try:
    ip_list[ip][protocol]
except KeyError:
    ip_list[ip][protocol] = []

# Append the port to the list
ip_list[ip][protocol].append(port)

with open(path.abspath('nmap.txt'), 'a') as f:
    sorted_ips = sorted(ip_list.items(), key=lambda item: inet_aton(item[0]))
    for ip, protocols in sorted_ips:
        udp_ports = ""
        tcp_ports = ""

        # Check to see if any UDP ports were found
        try:
            for port in protocols['udp']:
                udp_ports += port + ','
        except KeyError:
            pass

        # Check to see if any TCP ports were found
        try:
            for port in protocols['tcp']:
                tcp_ports += port + ','
        except KeyError:
            pass

        # Print IP and ports to file ready for NMap scan
        if udp_ports and tcp_ports:
            line = ip + ' -p U:' + udp_ports + 'T:' + tcp_ports

```

```
elif udp_ports:
    line = ip + ' -p U:' + udp_ports
elif tcp_ports:
    line = ip + ' -p T:' + tcp_ports
f.write(line + '\n')
```

Revision #4

Created 23 June 2024 20:19:12 by naruzkurai

Updated 23 June 2024 20:25:14 by naruzkurai