The Center for Cyber Defenders

Expanding Computer Security Knowledge

SAND2015-5714C

Network Host Discovery (NetHD)

Jeffrey Bigg and Anthony Dust – University of Illinois Urbana-Champaign

Project Mentor: Michael Stickland/5624

Problem Statement:

Red Team personnel utilize several reconnaissance tools to map the topology of a target network. This project explores methods for taking these varied tools and combining their results to create a powerful, unified tool. NetHD is an attempt to accomplish this task by creating a modular tool that unifies the results of various network reconnaissance tools into a usable, common data format.

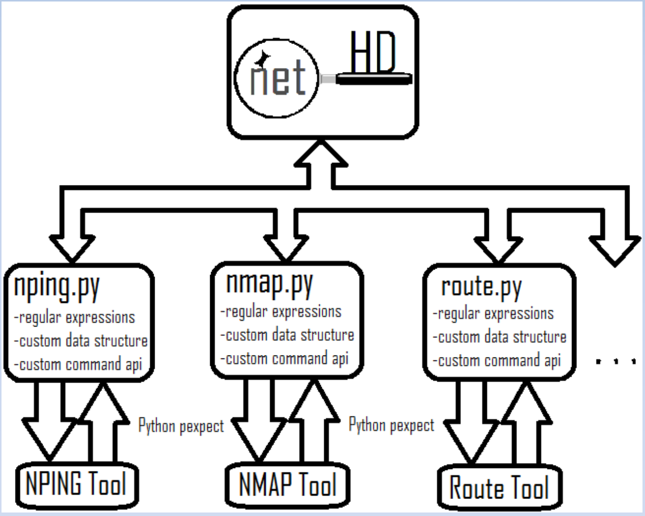


Figure 1: Project structure

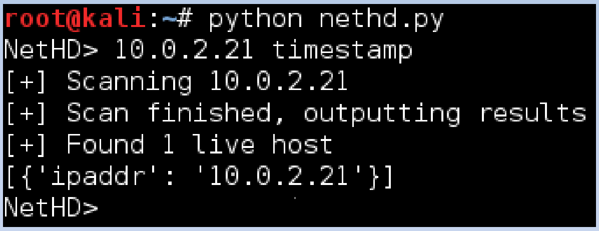
Approach:

- Construct various network topologies to map
- Create wrappers for reconnaissance tools
- Design a universal data structure for storing network mapping results
- Test the accuracy of the unified scan results

Results:

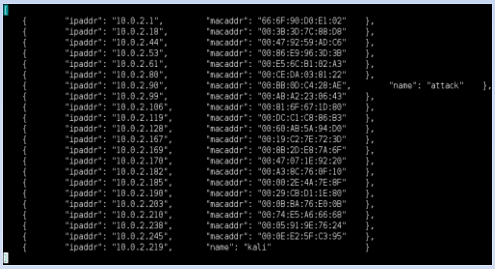
We created Python libraries, utilizing pexpect, to deploy Nmap, Nping, and route based on user commands (see Fig. 1 and Fig. 2).

The output is parsed and merged into our extensible custom format (see Fig. 3) which currently supports: Hostname, MAC Address, and IP Address. The output can be exported as a JSON file, and the data structure which supports this internally provides duplicate host detection and merging.



```
root@kali:~# python nethd.py
NetHD> 10.0.2.21 timestamp
[+] Scanning 10.0.2.21
[+] Scan finished, outputting results
[+] Found 1 live host
[{'ipaddr': '10.0.2.21'}]
NetHD>
```

Figure 2: 1 target, ICMP type 13 scan



```
[
    {       "ipaddr": "10.0.2.1",        "macaddr": "66:6F:90:D0:E1:02"    },
    {       "ipaddr": "10.0.2.18",       "macaddr": "00:3B:3D:7C:8B:D8"    },
    {       "ipaddr": "10.0.2.44",       "macaddr": "00:47:92:59:AD:C6"    },
    {       "ipaddr": "10.0.2.53",       "macaddr": "00:86:E9:96:3D:3B"    },
    {       "ipaddr": "10.0.2.61",       "macaddr": "00:E5:6C:B1:02:A3"    },
    {       "ipaddr": "10.0.2.80",       "macaddr": "00:CE:DA:03:81:22"    },
    {       "ipaddr": "10.0.2.90",       "macaddr": "00:BB:0D:C4:28:AE",       "name": "attack"    },
    {       "ipaddr": "10.0.2.99",       "macaddr": "00:AB:A2:23:06:43"    },
    {       "ipaddr": "10.0.2.106",      "macaddr": "00:81:6F:67:1D:80"    },
    {       "ipaddr": "10.0.2.119",      "macaddr": "00:DC:C1:C8:86:B3"    },
    {       "ipaddr": "10.0.2.128",      "macaddr": "00:60:AB:5A:94:D0"    },
    {       "ipaddr": "10.0.2.167",      "macaddr": "00:19:C2:7E:72:3D"    },
    {       "ipaddr": "10.0.2.169",      "macaddr": "00:8B:2D:E8:7A:6F"    },
    {       "ipaddr": "10.0.2.170",      "macaddr": "00:47:07:1E:92:20"    },
    {       "ipaddr": "10.0.2.182",      "macaddr": "00:A3:8C:76:0F:10"    },
    {       "ipaddr": "10.0.2.185",      "macaddr": "00:00:2E:4A:7E:8F"    },
    {       "ipaddr": "10.0.2.190",      "macaddr": "00:29:CB:D1:1E:80"    },
    {       "ipaddr": "10.0.2.203",      "macaddr": "00:0B:BA:76:E0:0B"    },
    {       "ipaddr": "10.0.2.210",      "macaddr": "00:74:E5:A6:66:68"    },
    {       "ipaddr": "10.0.2.238",      "macaddr": "00:05:91:9E:76:24"    },
    {       "ipaddr": "10.0.2.245",      "macaddr": "00:0E:E2:5F:C3:95"    },
    {       "ipaddr": "10.0.2.219",      "name": "kali"                    }
]
```

Figure 3: Sample nmap .py result

Future Work:

- Instrument additional tools
- Add support for new data fields
- Identify a host’s device type
- Uniquely identify one host with multiple NICs
- Develop a standard set of test networks for tool verification

Sandia National Laboratories is a multi-program laboratory operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin company, for the U.S. Department of Energy's National Nuclear Security Administration under con-