MUNI

Network Monitoring and Enumerating Vulnerabilities in Large Heterogeneous Networks

NOMS 2020

Martin Laštovička

Motivation

- Large heterogeneous networks
  - Many departments, Wi-Fi, BYOD, DHCP
- How to assess impact of a new vulnerability?
  - Critical vulnerability on a system we don’t have in our network
- Many approaches for discovering vulnerable hosts

Goals

1. How precise are network monitoring tools in recognizing software and its version on hosts in a computer network?
2. How precise are descriptions of vulnerabilities with regards to name and version of the vulnerable software?
3. How precisely can we estimate the number of vulnerable hosts for a given vulnerability?

Campus Network

- More than 40,000 users
- One /16 network segment of 65,535 IPv4 addresses
- ~19,000 unique IP addresses actively communicate each day
- 6.91k network flows/s (550 kpps) on average
- 11k flows per second (900 kpps) in rush hours

RQ1: How precise are network monitoring tools in recognizing software and its version on hosts in a computer network?

MUNI

Monitoring Tools

- Passive network monitoring
  - NetFlow fingerprinting
- Active scanning from internal network
  - Nmap
  - WhatWeb
- External scanner
  - Shodan

NetFlow Fingerprinting

- NOMS 2018 Passive OS Fingerprinting Methods in the Jungle of Wireless Networks
- NOMS 2020 Using TLS Fingerprints for OS Identification in Encrypted Traffic (yesterday ES)
- OS identification from
  - TCP/IP parameters
  - HTTP User-agent
  - Specific domain communication
  - TLS handshake

MUNI

NetFlow OS Identification Analysis

- Analyzed one day of traffic
- NetFlows from backbone network
- 18,018 hosts with at least one software identified

Vendor	Product	Version	Update	Edition	Count
✓	×	×	×	×	166
✓	✓	×	×	×	7,813
✓	✓	✓	×	×	10,039
✓	✓	✓	✓	×	0
✓	✓	✓	✓	✓	0

MUNI

Nmap Scan Settings

- Top 1000 ports, service identification (-sV -n -T5)
- Scanning point in the central server segment
- 16 hours 9 minutes
- 5,771 “host up”
  - But 3,152 with all ports closed/filtered

Nmap Scan

- 2,619 hosts with at least one port open
- 1,872 hosts with at least one software identified

Vendor	Product	Version	Update	Edition	Count
✓	×	×	×	×	0
✓	✓	×	×	×	252
✓	✓	✓	×	×	1,620
✓	✓	✓	✓	×	0
✓	✓	✓	✓	✓	0

WhatWeb Scan

- List of all registered domains (382 active hosts)
- 363 hosts with at least one software identified

Vendor	Product	Version	Update	Edition	Count
✓	×	×	×	×	3
✓	✓	×	×	×	56
✓	✓	✓	×	×	304
✓	✓	✓	✓	×	0
✓	✓	✓	✓	✓	0

Coverage of Monitoring Tools

- 18,749 active IP addresses
  - Had sent at least one UDP packet or TCP packet with SYN flag from campus network to the outside world
- Below is the percentage of hosts with at least one software identified by the methods

Method	Vendor	Product	Version	Update	Total
NetFlow	0.89 %	41.67 %	53.54 %	0.00 %	96.10 %
Nmap	0.00 %	1.34 %	8.64 %	0.00 %	9.98 %
WhatWeb	0.02 %	0.30 %	1.62 %	0.00 %	1.94 %

RQ2: How precise are descriptions of vulnerabilities with regards to name and version of the vulnerable software?

MUNI

CVE Analysis

- 1,441 vulnerabilities from 01/2019 to 03/2019
- 1,422 CVEs with CPE (Common Platform Enumeration)
- CPE version 2.2 used:

```
cpe:/<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>
```

- (CPE 2.3)

```
cpe:2.3:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>
:<sw_edition>:<target_sw>:<target_hw>:<other>
```


MUNI

CVE Analysis

Vendor	Product	Version	Update	Edition	Count
✓	*	*	×	×	0
✓	✓	*	×	×	184
✓	✓	✓	×	×	1,105
✓	✓	✓	✓	×	132
✓	✓	✓	✓	✓	1

RQ3: How precisely can we estimate the number of vulnerable hosts for a given vulnerability?

Mapping of CVEs to Hosts

- Matching CPE from CVE to identified software
  - Full match of CVE CPE and detected CPE
  - Match of the vendor, product, and version with CVE, including update and edition
  - detected vendor and product with CVE for a specific version
  - detected vendor with CVE for a product
- Shodan
  - Queried directly for all vulnerabilities found in the campus /16 network
- 223 CVEs matched to our hosts
- 40 unique CPEs used

Vulnerable Hosts

Method	Unique CPEs	Unique CVEs	CVEs with Attack Vector: Network	Hosts
NetFlow	71	221	118	17,418
Nmap	169	37	13	815
WhatWeb	223	29	29	136
Shodan	-	19	19	38

Most Common Vulnerabilities per Method

Method	Top CVE	CPE	NetFlow	Nmap	WhatWeb	Shodan
NetFlow	CVE-2019-0663	cpe:/o:microsoft:windows_10:- cpe:/o:microsoft:windows_7:-:sp1 cpe:/o:microsoft:windows_8.1:- ...	12,626	0	0	0
Nmap	CVE-2019-9003	cpe:/o:linux:linux_kernel	2,011	739	0	0
WhatWeb	CVE-2019-0190	cpe:/a:apache:http_server:2.4.37 cpe:/a:openssl:openssl	0	75	55	2
Shodan	CVE-2019-9024	cpe:/o:debian:debian_linux:9.0 cpe:/a:php:php	2,012	0	52	18

MUNI

Summary

- SW identification coverage ranges from 2 to 96 %
  - Even scan from internal server segment discovered only a fraction of active hosts
- Questionable usability of CVE with SW and version
  - i.e. Vulnerability in Microsoft Windows 10
- Passive methods are good for wide sweep
- Active methods for targeted confirmation

MUNI

MUNI