Network Security: Scan

Seungwon Shin, KAIST

some slides from Dr. Brett Tjaden
More about Scan
Scan Techniques

- Network scanning
  - where is a target?
  - which service is available on a target?
  - can I have more information?

- Vulnerability scanning
  - which vulnerable services are running on a target?
ICMP Scan

- ICMP protocol
  - used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached
  - several types
    - type 8
      - echo request
      - ping packet
    - type 13
      - timestamp request
    - type 15
      - information request
      - RARP, BOOTP (rarely used)
    - type 17
      - subnet address mask request
      - find the subnet mask used by the target host

ICMP packet format

<table>
<thead>
<tr>
<th>type</th>
<th>code</th>
<th>checksum</th>
<th>message-specific information</th>
</tr>
</thead>
</table>

32 bits

from nmap.org
ICMP Scan Example

- **Nmap**
  - send ping packet
  - not so effective

- **ICMPSnscan**
  - a bulk scanner that sends type 8, 13, 15, and 17 messages
  - example
    - `icmpscan -c -t 500 -r 1 192.168.1.0/24`
    - c: enable promiscuous mode
    - t: timeout for probe response (ms)
    - r: retries for each probe

- **xprobe2**
  - can do OS fingerprinting with ICMP
  - example
    - `xprobe2 -v 192.168.0.174`
xprobe2 example
How xprobe2 works

How to fingerprint

- use OS specific implementation of TCP/IP stack

14:42:36.105884 IP (tos 0x6, ECT(0), ttl 64, id 19475, offset 0, flags [DF], proto: ICMP (1), length: 84) 192.168.0.4 > 192.168.0.101: ICMP echo request, id 19639, seq 1, length 64

14:42:36.107486 IP (tos 0x0, ttl 128, id 59791, offset 0, flags [DF], proto: ICMP (1), length: 84) 192.168.0.101 > 192.168.0.4: ICMP echo reply, id 19639, seq 1, length 64

14:45:59.273678 IP (tos 0x6, ECT(0), ttl 64, id 49892, offset 0, flags [DF], proto: ICMP (1), length: 84) 192.168.0.4 > 192.168.0.100: ICMP echo request, id 22065, seq 1, length 64

14:45:59.275212 IP (tos 0x6, ECT(0), ttl 64, id 56932, offset 0, flags [none], proto: ICMP (1), length: 84) 192.168.0.100 > 192.168.0.4: ICMP echo reply, id 22065, seq 1, length 64
TCP Scan

- usual
  - `connect()` call scan
  - half-open TCP SYN scan
- kind of stealthy
  - inverse TCP flag scan
  - ACK flag scan
  - TCP fragmentation scan
- with the help of a third-party
  - FTP bounce
Inverse TCP flag

- F/W and IDS will detect (or record) a SYN packet sent to some sensitive network ports
  - e.g., port 80, 443, and etc
- An attacker can evade by sending
  - FIN probe packet (FIN flag)
  - XMAS probe (FIN, URG, and PUSH flag)
  - NULL probe (no flags)

TCP FIN packet to 80

- if open: no response
- if closed: RST/ACK

RFC 793: out of state packet to an open port - discard
FTP Bounce Scan

Why do we need this?

- hide an attacker

1. set up a connection
2. issue a PORT command
3. issue a LIST command
4. create a connection to the target
5. response from the target
6. deliver the results
FTP Bounce Scan

PORT 143.248.111.100:23
200 PORT command successful

LIST 143.248.111.100:23
150 Opening ASCII mode data connection for the list
226 transfer complete

LIST 143.248.111.100:23
425 Can’t build data connection: Connection refused

23 open

23 closed
Others

- Some more useful tools
  - whois
  - dig
  - nslookup
  - web search
  - and much more
Vulnerability Scan

- **Vulnerability scanner**
  - an automated tool that scans hosts and networks for known vulnerabilities and weaknesses
  - find which host is vulnerable to what

- **Examples**
  - NESSUS
    - now commercial product
  - OpenVAS
    - fork of NESSUS, open source
  - Retina
    - commercial product
Vulnerability Scan

How it works

Similar to virus scanning software:

- Contain a database of vulnerability signatures that the tool searches for on a target system
- Cannot find vulnerabilities not in the database
  - New vulnerabilities are discovered often
  - Vulnerability database must be updated regularly
Vulnerability Scan

Find what

- Network vulnerabilities
- Host-based (OS) vulnerabilities
  - Misconfigured file permissions
  - Open services
  - Missing patches
  - Vulnerabilities in commonly exploited applications
    - Web, DNS, and mail servers
Vulnerability Scan

Vulnerability Database → GUI → Scanning Engine → Knowledge Base → Results → target

- target
- target
- target
- target
OpenVAS

- www.openvas.org
Case Study
Interesting Research Work

- A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan
  - written by Ang Cui and Salvatore J. Stolfo
    - Columbia University
  - Published in ACSAC 2012
    - Student Best Paper
Problem Domain and Goal

- Embedded Devices have been known that they are Insecure and available as a source for new, stealthy botnets.

- Then, how to know if it is true?
  - A global scan method can be used in getting some clues.
Approach

Scan the world
Scan the world’s largest
  Residential ISPs
  Commercial ISPs
  EDU, GOV etc
Scan in
  United States
  Asia
  Europe

Identify Embedded Devices
  cisco-IOS
  level_15_access
  Linksys SPA Configuration
  Linksys PAP2 Configuration
  SpeedStream Router Configurator
  DD-WRT Control Panel
  |  web_cisco-web
  |  web_cisco-web
  |  web_linksys-spa
  |  web_linksys-pap2
  |  web_speedstream
  |  web_ddwrt

Try the default password

```json
cisco

root:
  username_prompt: ['sername:']
  username: ['cisco']
  askuser: true
  passstr: ['password:']
  incorrect: ['sername, a$ssword']
  success: ['\$', '\#', '>']
  passwords: ['cisco']
  deviceType: cisco
  linesep: ''
```
Scan

- Recognizance
  - scan large portions of the internet
  - port 23 (telnet) and 80 (http)

- Identification
  - try to connect all telnet and http servers
  - detect their manufacturer and model of the device

- Verification
  - try to log in with the default password
Distribution of vulnerable embedded devices

(total number: 540,435)
Result

Distribution of vulnerable embedded devices (types)
Result
Why is this important?

– Router Exploitation
  • DIK (Da IOS Rootkit, Sebastian Muniz)
  • Router Transit Vulnerabilities (Felix Linder)
  • Reliable Cisco IOS Exploit (Felix Linder)

– Router Botnet
  • Network Bluepill
    – http://dronebl.org/blog
  • Keiten Bot
    – Helel Mod 1.0 – Ezba’ Elohim
    – Runs on D-link routers
    – http://packetstormsecurity.nl/irc/kaiten.c
When Firmware Modifications Attack: A Case Study of Embedded Exploitation
NDSS, 2013

The State of Embedded-Device Security (Spoiler Alert: It's Bad)

Shodan!
Shodan

- It is a search engine that allows you to look for devices connected to the internet
  - mostly embedded devices
    - webcam, wireless AP, and etc
- How to provide search results?
  - scanning networks
Shodan

EXPOSE ONLINE DEVICES.

WEBCAMs. ROUTers.
POWER PLANTS. iPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR  FREE SIGN UP

Popular Search Queries: Router w/ Default Info - Routers that give their default username/password as admin:1234 in their banner.

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS
Shodan pinpoints shoddy industrial controls.
It greatly lowers the technical bar needed to canvas the Internet...
"Shodan for Penetration Testers" presented at DEF CON 18
It's a reminder to many to know what's on your network...

The A Register  threatpost  DEFCON  dark READING
Shodan

Top Countries:
- Korea, Republic of: 4,242
- Hong Kong: 27
- Japan: 10
- China: 8
- United States: 3

Top Services:
- FTP: 3,819
- NetBIOS: 320
- SSH: 41
- NAS Web Interfaces: 25
- UPnP: 18

Top Organizations:
- Korea Telecom: 2,088
- SK Broadband: 1,135
- LG Powercom: 358
- POWERCOM: 161
- Powercom: 30

Top Operating Systems:
- Linux 2.6.x: 1

Total results: 4,297

27.117.6.131
Tbroad Nakdong Broadcasting co., Ltd
Added on 2016-05-13 19:05:49 GMT
- Korea, Republic of, Suwon

125.128.173.215
Korea Telecom
Added on 2016-05-13 19:05:30 GMT
- Korea, Republic of

1.225.56.189
SK Broadband
Added on 2016-05-13 19:00:39 GMT
- Korea, Republic of

118.35.97.141
Korea Telecom
Added on 2016-05-13 19:00:15 GMT
- Korea, Republic of