Network Security: Scan

Seungwon Shin, KAIST

some slides from Dr. Brett Tjaden

More about Scan

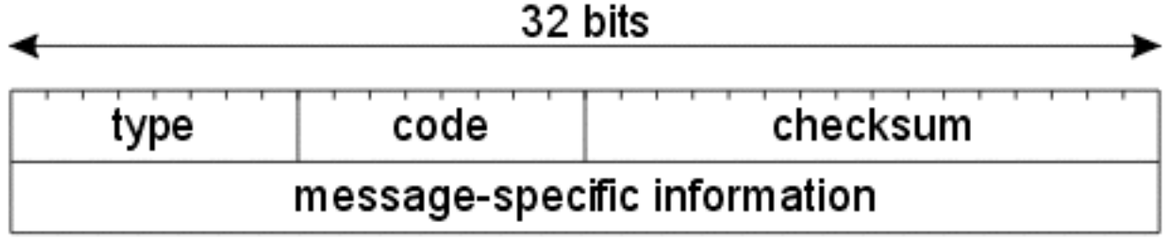
Scan Techniques

- 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



from nmap.org

ICMP Scan Example

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

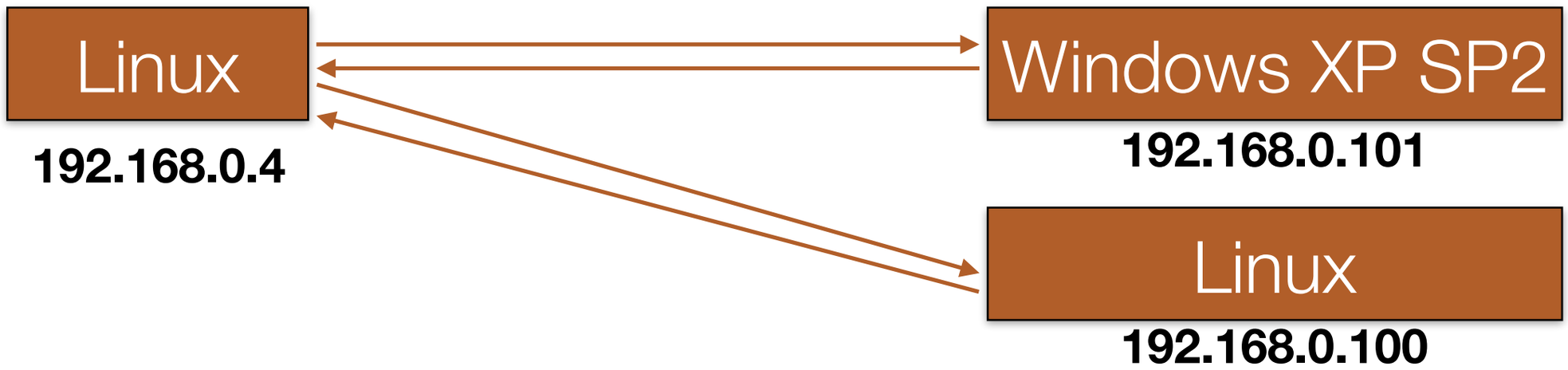
```
claude@ubuntu: ~
Name:   syssec.kaist.ac.kr
Address: 143.248.57.220

claude@ubuntu:~$ sudo xprobe2 -v 143.248.57.220

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 143.248.57.220
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 143.248.57.220. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 143.248.57.220. Module test failed
[-] No distance calculation. 143.248.57.220 appears to be dead or no ports known
[+] Host: 143.248.57.220 is up (Guess probability: 50%)
[+] Target: 143.248.57.220 is alive. Round-Trip Time: 0.00482 sec
[+] Selected safe Round-Trip Time value is: 0.00964 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 143.248.57.220 Running OS: "Microsoft Windows 2000 Workstation" (Guess probability: 83%)
[+] Other guesses:
[+] Host 143.248.57.220 Running OS: "Microsoft Windows 2000 Workstation SP4" (Guess probability: 83%)
[+] Host 143.248.57.220 Running OS: "HP JetDirect ROM F.08.08 EEPROM F.08.20" (Guess probability: 83%)
[+] Host 143.248.57.220 Running OS: "Microsoft Windows XP SP1" (Guess probability: 83%)
[+] Host 143.248.57.220 Running OS: "HP JetDirect ROM F.08.08 EEPROM F.08.05" (Guess probability: 83%)
[+] Host 143.248.57.220 Running OS: "HP JetDirect ROM H.07.15 EEPROM H.08.20" (Guess probability: 83%)
[+] Host 143.248.57.220 Running OS: "HP JetDirect ROM G.07.19 EEPROM G.08.03" (Guess probability: 83%)
[+] Host 143.248.57.220 Running OS: "Microsoft Windows NT 4 Workstation Service Pack 6a" (Guess probability: 83%)
[+] Host 143.248.57.220 Running OS: "HP JetDirect ROM G.06.00 EEPROM G.06.00" (Guess probability: 83%)
[+] Host 143.248.57.220 Running OS: "HP JetDirect ROM G.05.34 EEPROM G.05.35" (Guess probability: 83%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
claude@ubuntu:~$
```

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

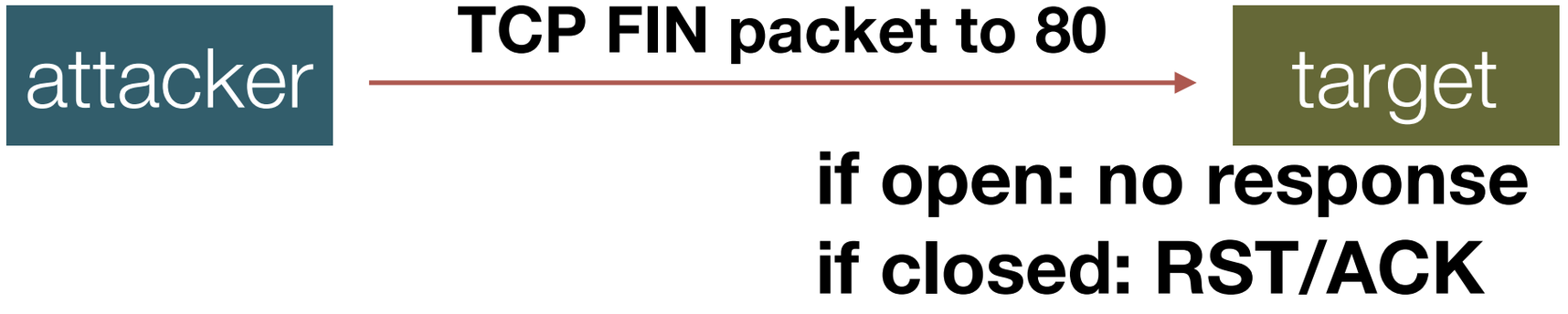
14:45:59.275212 IP (tos 0x6,**ECT(0)**, **ttl 64**, id 56932, offset 0, flags [none], proto: ICMP (1), length: 84) ***192.168.0.100 > 192.168.0.4***: ICMP echo reply, id 22065, seq 1, length 64

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

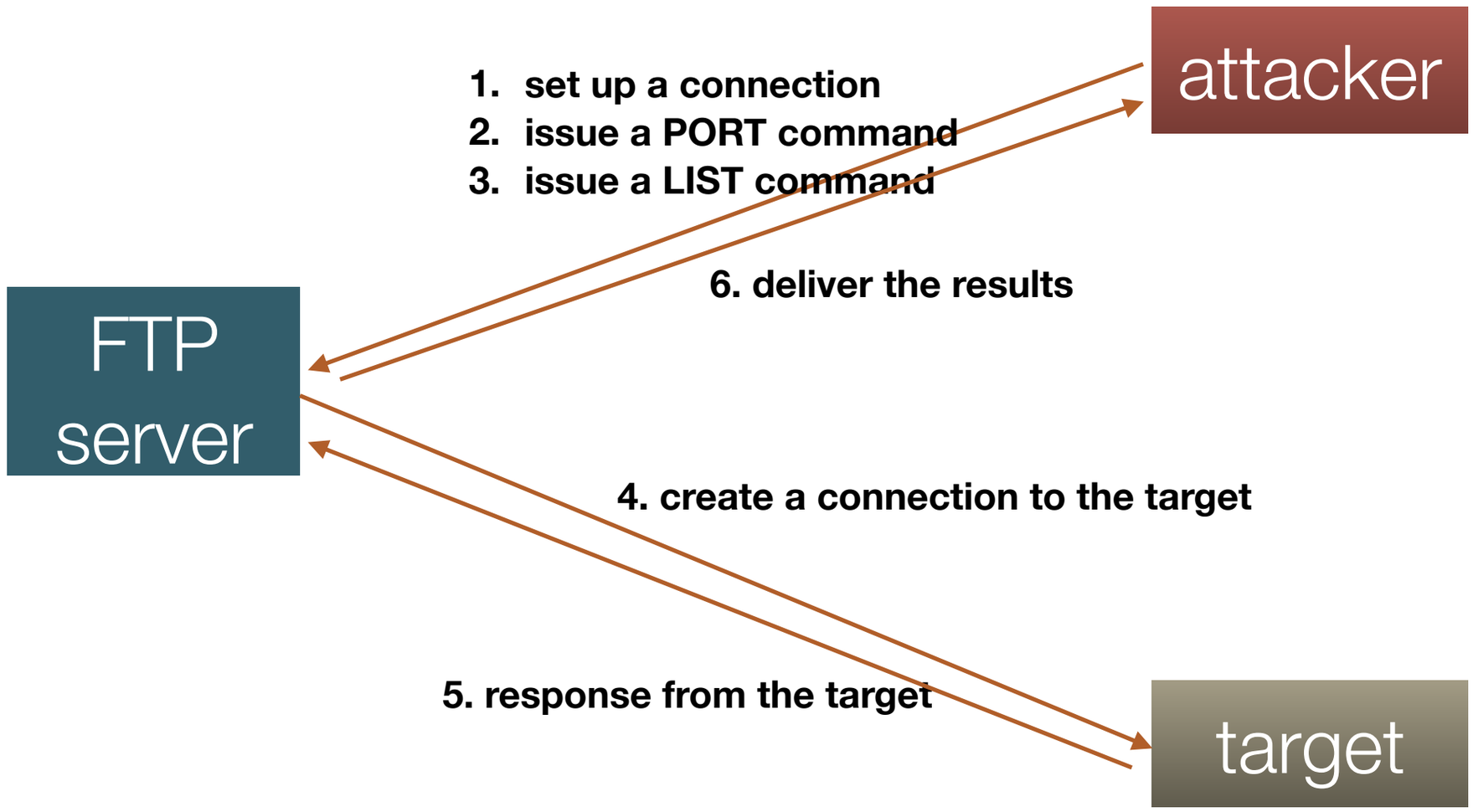
- F/W and IDS will detect (or record) a SYN packet sent to some sensitive network ports
  - e.g., port 80, 443, and etc
- An attacker can evade by sending
  - FIN probe packet (FIN flag)
  - XMAS probe (FIN, URG, and PUSH flag)
  - NULL probe (no flags)



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

FTP Bounce Scan

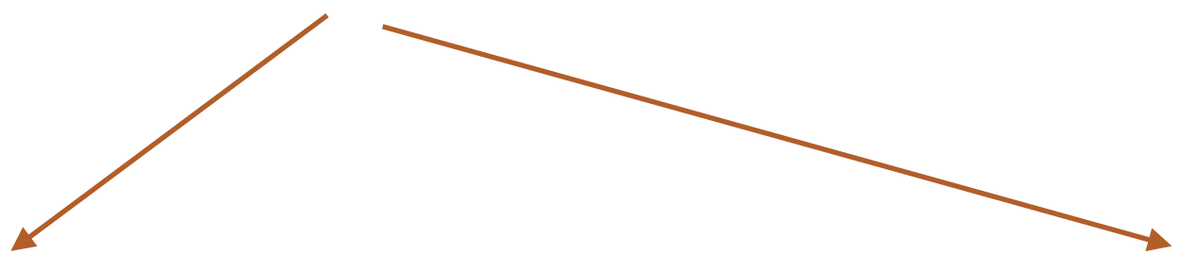
- Why do we need this?
  - hide an attacker



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

23 open

LIST 143.248.111.100:23

425 Can’t build data connection: Connection refused

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

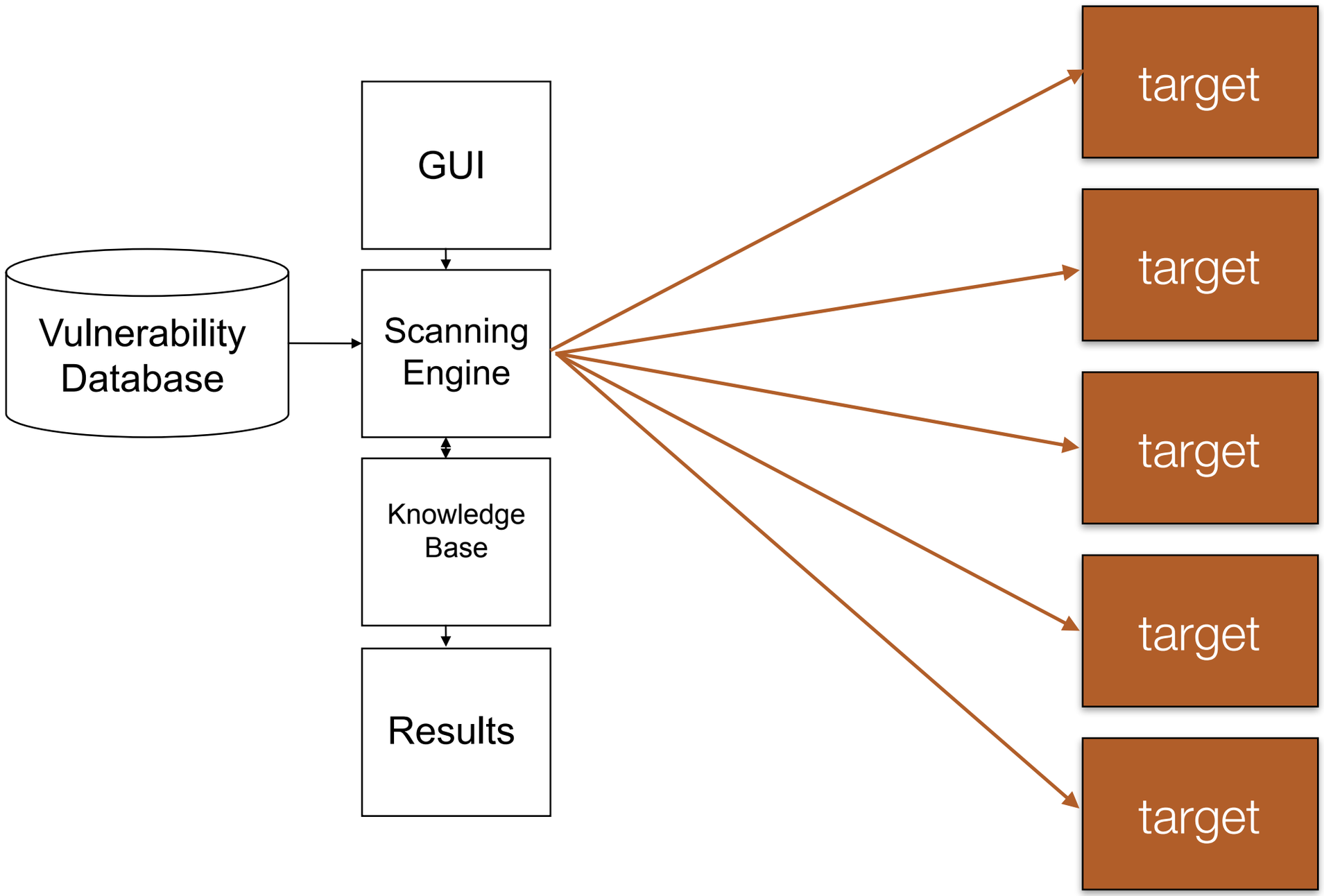
Vulnerability Scan

- 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

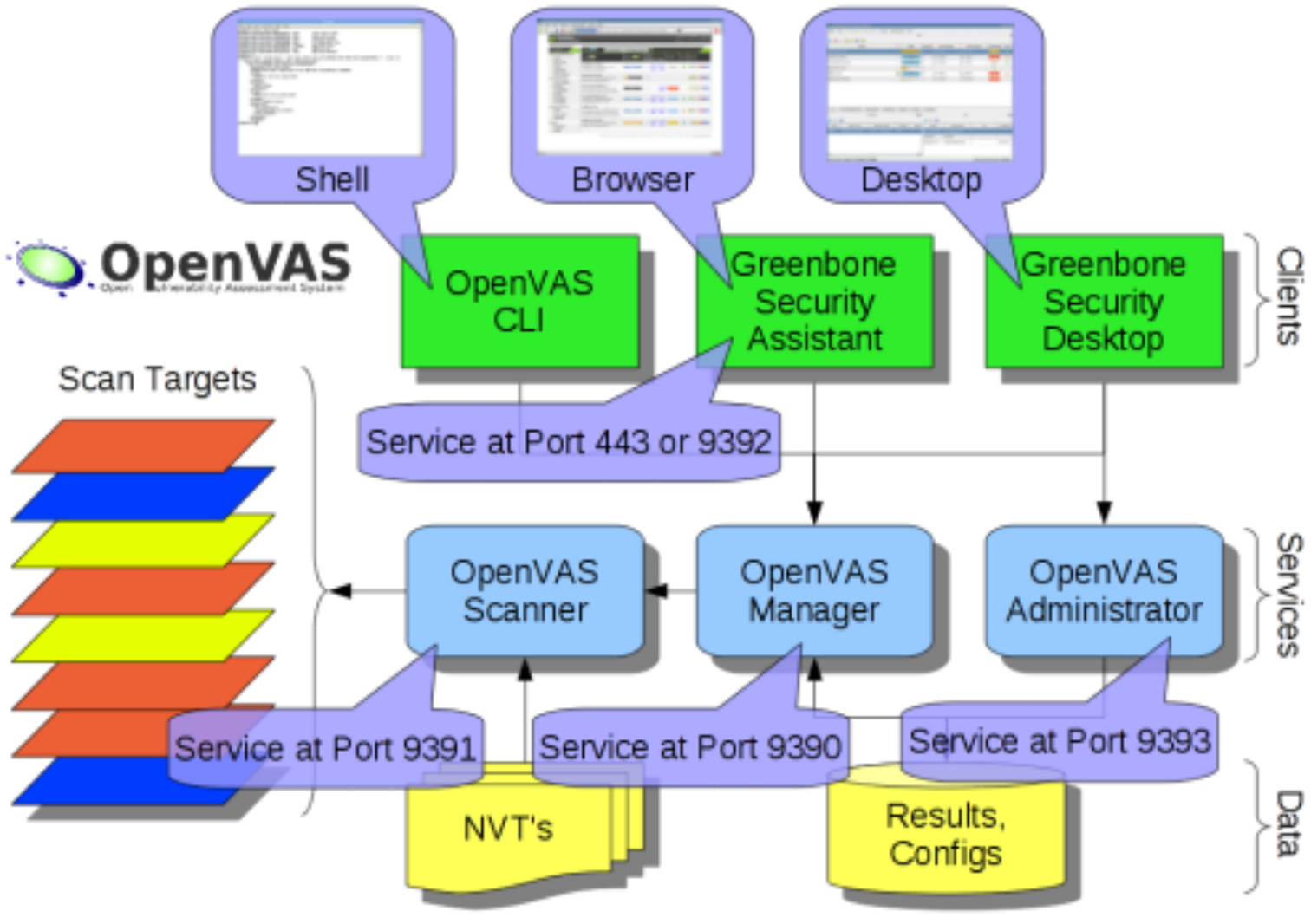
- Find what
  - Network vulnerabilities
  - Host-based (OS) vulnerabilities
    - Misconfigured file permissions
    - Open services
    - Missing patches
    - Vulnerabilities in commonly exploited applications
      - Web, DNS, and mail servers

Vulnerability Scan



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	web_cisco-web
level_15_access	web_cisco-web
Linksys SPA Configuration	web_linksys-spa
Linksys PAP2 Configuration	web_linksys-pap2
SpeedStream Router Configurator	web_speedstream
DD-WRT Control Panel	web_ddwrt

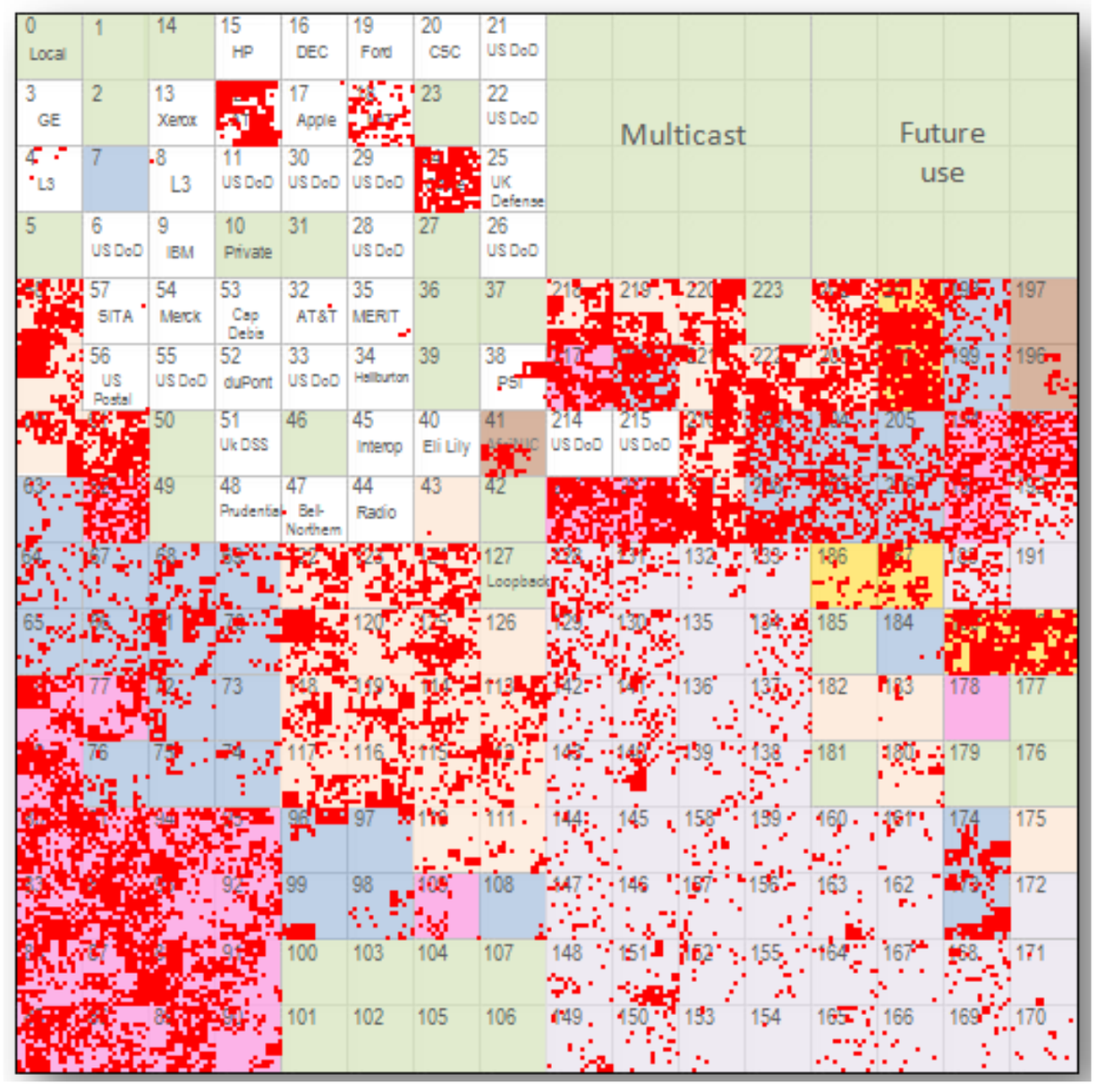
Try the default password

```
root:
    username_prompt: ['sername:']
    username: ['cisco']
    askuser: true
    passstr: ['assword:']
    incorrect: [sername, assword]
    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

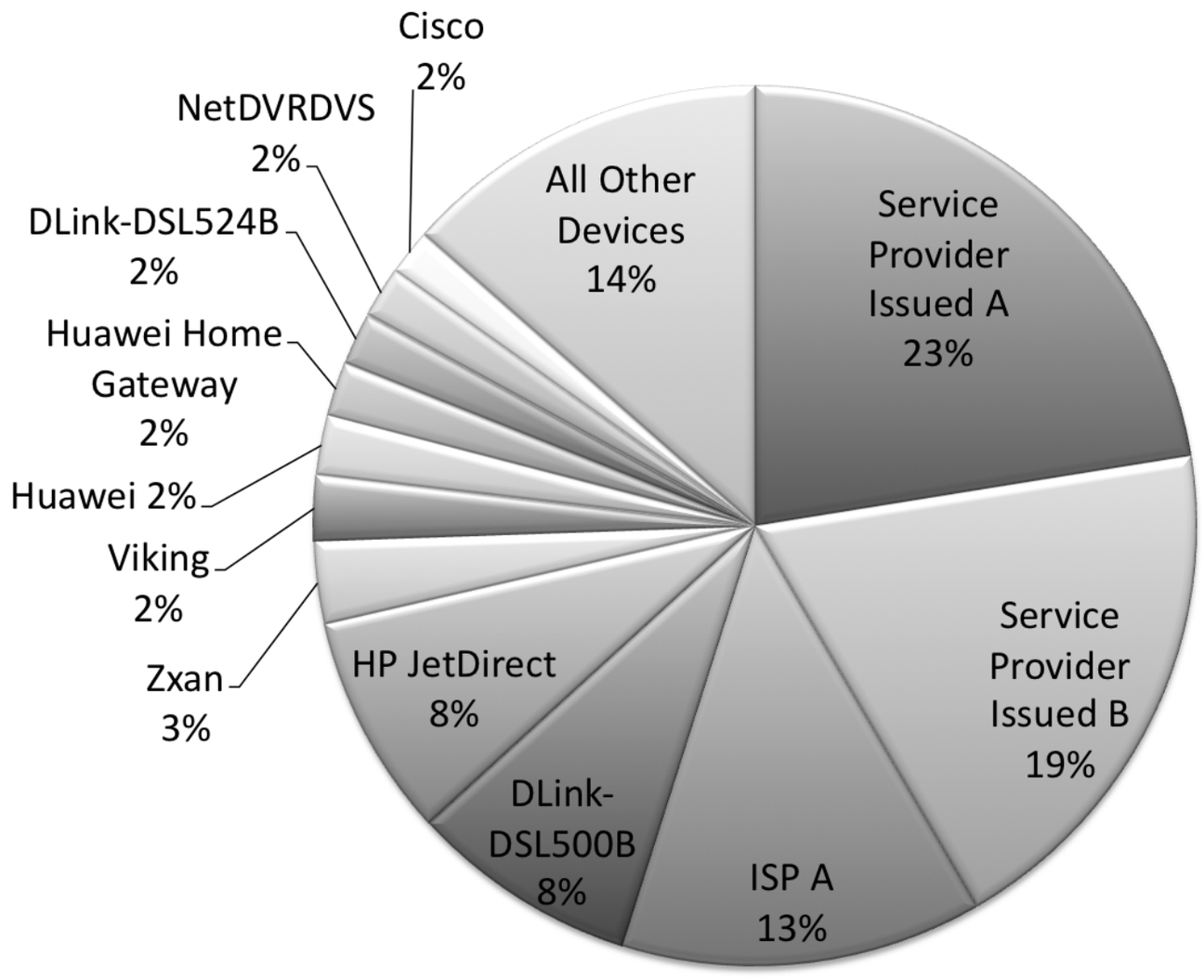
Result



Distribution of vulnerable embedded devices

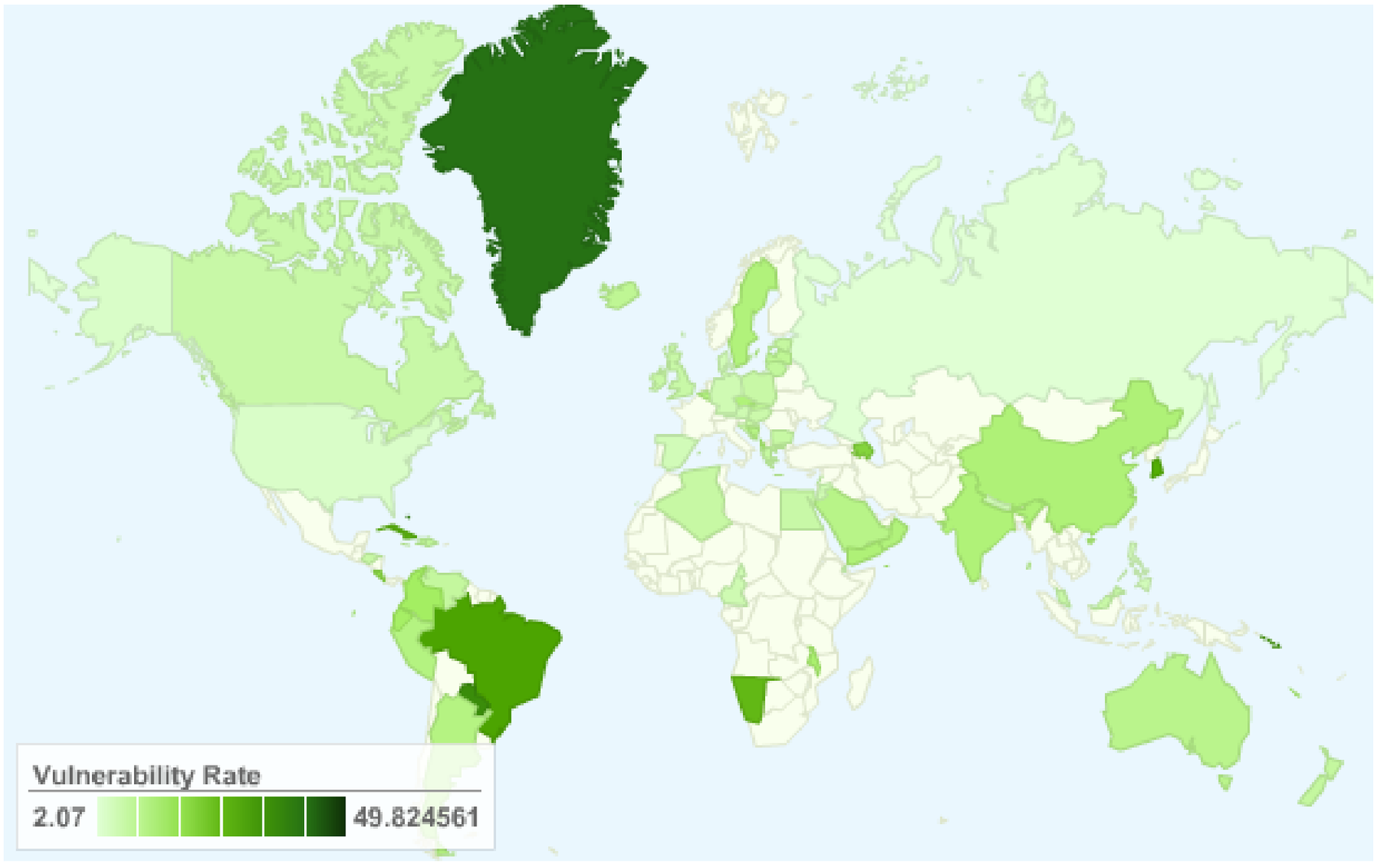
total number: 540,435

Result



Distribution of vulnerable embedded devices (types)

Result



Why is this important?

- Router Exploitation
  - DIK (Da IOS Rootkit, Sebastian Muniz)
    - http://eusecwest.com/esw08/esw08-muniz.pdf
  - Router Transit Vulnerabilities (Felix Linder)
    - http://www.blackhat.com/presentations/bh-usa-09/LINDNER/BHUSA09-Lindner-RouterExploit-SLIDES.pdf
  - Reliable Cisco IOS Exploit (Felix Linder)
    - http://www.phenoelit-us.org/stuff/FX_Phenoelit_25c3_Cisco_IOS.pdf
- 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

Some Extension

- When Firmware Modifications Attack: A Case Study of Embedded Exploitation
  - NDSS, 2013
- The State of Embedded-Device Security (Spoiler Alert: It's Bad)
  - IEEE S&P Magazine, 2012
- Shodan!

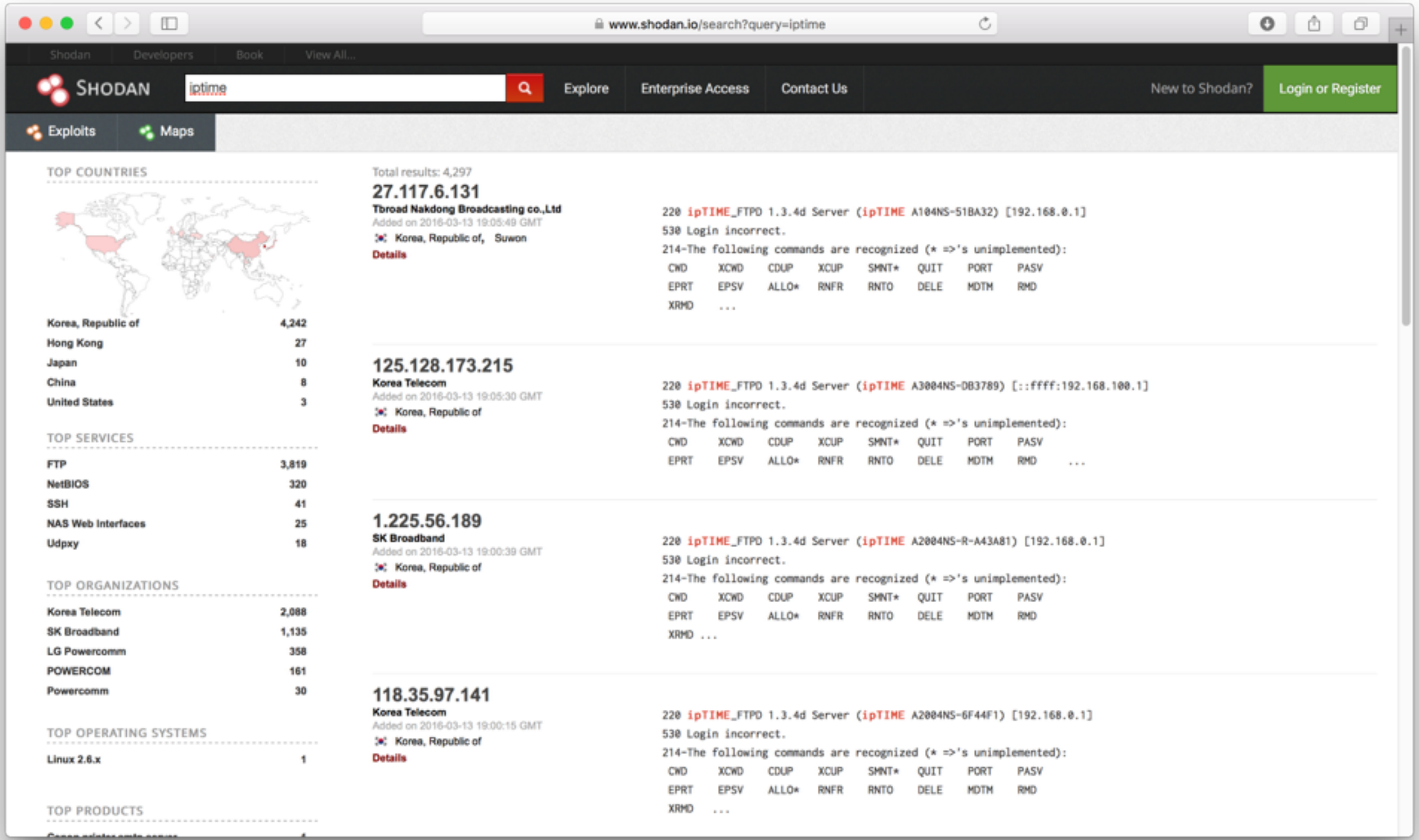
Shodan

- 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


www.shodanhq.com
DuckDuckGo
Shodan
Exploits
Scanhub
Maps
Blog
Anniversary Promotion
Settings
Logout
Buy
SHODAN
Search
Home
Search Directory
Data Analytics/ Exports
Developer Center
Labs
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...

Shodan


www.shodan.io/search?query=iptime
Shodan
Developers
Book
View All...
SHODAN
iptime
Explore
Enterprise Access
Contact Us
New to Shodan?
Login or Register
Exploits
Maps
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
Udpxy 18
TOP ORGANIZATIONS
Korea Telecom 2,088
SK Broadband 1,135
LG Powercomm 358
POWERCOM 161
Powercomm 30
TOP OPERATING SYSTEMS
Linux 2.6.x 1
TOP PRODUCTS
Total results: 4,297
27.117.6.131
Tbroad Nakdong Broadcasting co.,Ltd
Added on 2016-03-13 19:05:49 GMT
Korea, Republic of, Suwon
Details
220 ipTIME_FTPD 1.3.4d Server (ipTIME A104NS-51BA32) [192.168.0.1]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV
EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD
XRMD ...
125.128.173.215
Korea Telecom
Added on 2016-03-13 19:05:30 GMT
Korea, Republic of
Details
220 ipTIME_FTPD 1.3.4d Server (ipTIME A3004NS-DB3789) [::ffff:192.168.100.1]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV
EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD ...
1.225.56.189
SK Broadband
Added on 2016-03-13 19:00:39 GMT
Korea, Republic of
Details
220 ipTIME_FTPD 1.3.4d Server (ipTIME A2004NS-R-A43A81) [192.168.0.1]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV
EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD
XRMD ...
118.35.97.141
Korea Telecom
Added on 2016-03-13 19:00:15 GMT
Korea, Republic of
Details
220 ipTIME_FTPD 1.3.4d Server (ipTIME A2004NS-6F44F1) [192.168.0.1]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV
EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD
XRMD ...