

CSE508 Network Security

10/31/2017

Reconnaissance and Scanning

Michalis Polychronakis
Stony Brook University

Information Gathering

First step of an attacker: learn as much about a particular target as possible

human, system, organization, ...

Dependencies and third-party interactions are also important

Example: the Target 2013 breach was achieved through the compromise of a third-party HVAC vendor who had access to the internal network

Peripheral or “forgotten” systems are often less secure than publicized web, application server, and mail endpoints

Every piece of information counts!



Passive reconnaissance: no direct interaction with the target system

- Information gathering from public sources

- Passive network eavesdropping

- Dumpster diving (e.g., recover data from discarded hard disks)

- Information leakage (e.g., through social engineering)

Active reconnaissance: attacker's activities can be directly detected and logged

- Network scanning

- Service enumeration

- OS and service fingerprinting/probing

OSINT (Open-source Intelligence Gathering)

Intelligence collected from publicly available sources

As opposed to covert or clandestine sources

Wide variety of information and sources

Search engines: public documents, forgotten web pages, exposed login interfaces, dashboards, historical data, ...

Public data: courthouse documents, tax forms, budgets, ...

Media: articles, interviews, blog posts, ...

Social media: LinkedIn/Facebook/Twitter/etc., mailing lists, ...

Professional/academic sources: reports, presentations, ...

Metadata: documents, EXIF, executables, email headers, ...

...

Search Engines

Google, Bing, Yandex, Baidu, ...

Refined searches for certain kinds of information ("Google-Fu")

Useful operators: `intext`, `intitle`, `inurl`, `filetype`, `site`

Netcraft: uptime and web server info

Internet Archive's Wayback Machine: old site versions

Google/Yahoo groups: sysadm questions, gossip, ...

LinkedIn: persons within an organization, interests, ...

Qualys' SSL report: SSL configuration of public web servers

Many more: phone directories, "people" search, gov/state databases, dark web search, ...



Site report for www.cs.stonybrook.edu

Netcraft Extension

- Home
- Download Now!**
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Protection for TLDs against Phishing and Malware
- Deceptive Domain Score
- Bank Fraud Detection
- Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

- Installing the Extension
- Using the Extension
- Getting the Most
- Reporting a Phish

Lookup another URL:

 Share: [f](#) [t](#) [in](#) [g+](#) [y](#) [v](#)

Background

Site title	SBU - Computer Science Department - HOME	Date first seen	June 2005
Site rank	428532	Primary language	English
Description	Not Present		
Keywords	Not Present		

Network

Site	http://www.cs.stonybrook.edu	Netblock Owner	State University of New York at Stony Brook
Domain	stonybrook.edu	Nameserver	nocnoc.stonybrook.edu
IP address	130.245.27.2	DNS admin	dns@noc.stonybrook.edu
IPv6 address	Not Present	Reverse DNS	www.cs.stonybrook.edu
Domain registrar	educause.net	Nameserver organisation	whois.educause.net
Organisation	State University of New York/Stony Brook, Stony Brook University, Stony Brook, 11794-2630, United States	Hosting company	State University of New York/Stony Brook
Top Level Domain	Educational entities (.edu)	DNS Security Extensions	unknown
Hosting country	US		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
State University of New York at Stony Brook 247 ECC Building Stony Brook NY US 11794-2620	130.245.27.2	Linux	Apache/2.2.22 Ubuntu	9-Dec-2015
State University of New York at Stony Brook 247 ECC Building Stony Brook NY US 11794-2620	130.245.27.2	Linux	Apache	5-Aug-2014
State University of New York at Stony Brook 247 ECC Building Stony Brook NY US 11794-2620	130.245.27.2	Linux	Apache/2.2.3 Red Hat	25-Apr-2010
State University of New York at Stony Brook 247 ECC Building Stony Brook NY US 11794-2620	130.245.27.2	Solaris	Netscape-Enterprise/3.5.1	4-Apr-2005

Security

Netcraft Risk Rating [FAQ]	0/10
----------------------------	------



inurl:"sap-system-login"



Sign in

All

Images

News

Videos

Shopping

More ▾

Search tools



About 478 results (0.17 seconds)

Logon - SAP Web Application Server - Consumers Energyhttps://www.consumersenergy.com/.../hrrcf_a_startpa... ▾ Consumers Energy ▾**Configure Automatic SAP System Login with sapshcut - ITsiti**<itsiti.com/configure-automatic-sap-system-login-with-sapshcut> ▾

Please make sure that you already insert all your SAP system configuration in your SAPGUI shortcut (normally in desktop). To test the SAP system with no ...

Logon - SAP Web Application Server<https://suppliers.danfoss.com/?sap-system-login-oninputprocessing...> ▾**LOGIN تسجيل الدخول - SAP Web Application Server**https://jobs.aramco.com/.../hrrcf_a_reg_applwizard_ext?sap-system-logi... ▾**Logon - SAP Web Application Server**<extranet.fater.it:8003/.../bbpstart/?sap-system-login...> - Translate this page**Logon - Infosys Careers Web Application**https://careers.infosys.com/.../zhrrcf_a_startpage_row_lateral?sap-system... ▾**Logon - SAP Web Application Server - Oak Ridge National ...**https://recruiting.ornl.gov/.../zornl_a_startpage_ext_cand?sap-system-log... ▾**Anmeldung - SAP Web Application Server**https://online-hr.zf.com/.../hrrcf_a_... ▾ Translate this page ZF Friedrichshafen ▾**Logon - Mol**<https://recruiting.mol.hu/.../sap/system/login.htm?> ▾ Translate this page



intitle:"RouterOS" intitle:"configuration page" intext:"You have connected to



Sign in

All

Videos

Images

Shopping

News

More ▾

Search tools



About 363 results (0.21 seconds)

RouterOS router configuration page

ns.dacogr.com/ ▾

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator. User:

RouterOS router configuration page

oakamyan.muk.ac.ir/ ▾

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

RouterOS router configuration page

dakorwest.com/ ▾

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

RouterOS router configuration page

191.36.165.228/ ▾

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator. Select action ...

RouterOS router configuration page

95.142.143.47/ ▾

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator. Select action:.

RouterOS router configuration page - Catalog Software

www.catalogsoftware.org/get/dl/467194/ ▾

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.



"Password=" inurl:web.config -intext:web.config ext:config



Sign in

All

Videos

News

Images

Shopping

More ▾

Search tools



About 728 results (0.20 seconds)

web.config

ftp.mvaonline.com/partners.mvacolombia.com/wwwroot/web.config ▾
... connectionString="Data Source=ns1.nightshade.arvix.com;Initial Catalog=
dnn_mva;User ID=cballesteros;Password=[REDACTED]" providerName="System.

Copy of web.config - EarSinus.com

earsinus.com/new/Copy%20of%20web.config ▾
... the provider is specified passwordAttemptThreshold="int" The number of failed
password attempts, or failed password answer attempts that are allowed before ...

Web.config

ftp://60.250.85.148/StreamStore/WG/WebService/Web.config ▾
C:\wra10\FCT FcPumps.xml WaterLevel.xml Data Source=127.0.0.1;Initial
Catalog=River;User ID=sa;Password=[REDACTED]

web.config - Axis HR

www.axishrpro.co.uk/wwwroot/web.config ▾
SQLExpress;Database=hrpro;User ID=hrpro;Password=[REDACTED] /> </connectionStrings>
<appSettings> <add key="SQLServerConn" value="Server=.

D:\IMG_Catalogazione\ server=192.168.0.157 ...

ftp://37.186.241.19/InformFTP/pub/RussoM/.../marubi.../Web.Config ▾
D:\IMG_Catalogazione\ server=192.168.0.157;Trusted_Connection=false;User
ID=sa;Password=[REDACTED] Initial Catalog=marubi_web_cp; server=192.168.0.157 ...

web.config - PASA

www.pasaweb.com/forum/web.config ▾
... during which failed password attempts and failed password answer attempts are
tracked enablePasswordRetrieval="[true|false]" Should the provider support ...

[Home](#)[Exploits](#)[Shellcode](#)[Papers](#)[Google Hacking Database](#)[Submit](#)[Search](#)

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category ▼

Search

SEARCH

Date	Title	Category
2016-03-24	intitle:vood act=index Gateway >Login	Pages containing login portals
2016-03-24	intext:"powered by webcamXP 5"	Various Online Devices
2016-03-23	intitle:"VOOD - Welcome to Vood Residential Gateway >Login"	Pages containing login portals
2016-03-23	intitle:"Residential Gateway Configuration:" intext:"Cable Modem Information."	Various Online Devices
2016-03-23	intitle:"Login Page" intext:"Phone Adapter Configuration Utility"	Pages containing login portals
2016-03-22	(intext:"index of /.git") ("parent directory")	Sensitive Directories
2016-03-16	inurl:/sap/bc/webdynpro/sap/ "sap-system-login-oninputprocessing"	Pages containing login portals
2016-03-14	inurl:"sap-system-login"	Pages containing login portals
2016-03-14	inurl:"sap/hrrcf_a_startpage_ext_cand" inurl:"sap/hrrcf_a_pw_via_email_extern"	Pages containing login portals
2016-03-14	intitle:"Logon - SAP Web Application Server"	Pages containing login portals

Non-technical Information

Information about persons, operations, behaviors, is useful for targeted attacks 

Spear phishing: messages that appear to come from trusted sources

Watering hole attacks: target the members of a group by infecting websites they are known to regularly visit

Social networks, corporate websites, partners/third-parties, mailing lists, impersonation, social engineering, ...

LinkedIn, Twitter, Facebook, Google+, Instagram, Glassdoor, GitHub, Stackoverflow, ...

Public actions may also reveal actionable information

Example: a system administrator of a particular company asks on ServerFault how to secure Nginx 

TheHarvester <https://github.com/laramies/theHarvester>

[illegible]

What is this?

.....

theHarvester is a tool for gathering e-mail accounts, subdomain names, virtual hosts, open ports/ banners, and employee names from different public sources (search engines, pgp key servers).

Is a really simple tool, but very effective for the early stages of a penetration test or just to know the visibility of your company in the Internet.

Recon-ng <https://bitbucket.org/LaNMaSteR53/recon-ng>

[illegible]

Discover <https://github.com/leebaird/discover>

DISCOVER

By Lee Baird

RECON

1. Domain
2. Person
3. Parse salesforce

SCANNING

4. Generate target list
5. CIDR
6. List
7. IP, range, or URL

WEB

8. Open multiple tabs in Firefox
9. Nikto
10. SSL

MISC

11. Crack WiFi
12. Parse XML
13. Generate a malicious payload
14. Start a Metasploit listener
15. Update
16. Exit

Choice:

SpiderFoot <http://www.spiderfoot.net/>



SpiderFoot

New Scan

Scans

Settings

About

Zeus IP: 92.██████████226

Status

Browse

Graph

Scan Settings

Log



Search...



◆ Type	◆ Unique Data Elements	◆ Total Data Elements	◆ Last Data Element
Affiliate - Internet Name	24	24	2015-04-13 01:00:57
Affiliate - IP Address	22	22	2015-04-13 01:00:57
BGP AS Membership	1	1	2015-04-13 01:01:00
BGP AS Peer	103	103	2015-04-13 01:02:32
DNS TXT Record	1	1	2015-04-13 01:00:14
Domain Name	1	1	2015-04-13 01:00:08
Domain Whois	1	1	2015-04-13 01:00:14
Email Gateway (DNS 'MX' Records)	1	1	2015-04-13 01:00:14
HTTP Headers	2	2	2015-04-13 01:00:35
HTTP Status Code	1	2	2015-04-13 01:00:35
Internet Name	3	3	2015-04-13 01:00:34
IP Address	1	2	2015-04-13 01:00:07
Linked URL - External	69	72	2015-04-13 01:00:51
Linked URL - Internal	2	2	2015-04-13 01:00:35
Name Server (DNS 'NS' Records)	2	2	2015-04-13 01:00:14

WHOIS

Protocol for querying databases with registration information about assignees of internet resources

IP address blocks, domain names, and autonomous systems

Top registries: AFRINIC, APNIC, ARIN, IANA, ICANN, LACNIC, NRO, RIPE, InterNic

whois command-line utility

```
# whois stonybrook.edu
```

```
# whois 130.245.27.2
```

Registrars and third-party services provide web interfaces

Useful information

1. Registrar information, domain creation/expiration dates, primary DNS name servers associated with the domain
2. Registrant information such as First Name, Last Name, Organization, physical address, phone number, and e-mail address
3. Assigned domain administrator, billing contact, technical contact

DNS

Valuable information about individual hosts

- IP addresses (A, AAAA) of certain domains

- Name (NS) and mail (MX) servers of a domain

- Name aliases (CNAME) and reverse mappings (PTR)

Other useful records

- SRV: generic service locator (protocol, host, port) for domain services (e.g., Kerberos, LDAP, SIP, XMPP)

- TXT: SPF, DKIM, DMARC, and other custom information

- HINFO: CPU, OS, and other host-related information

Various utilities: nslookup, dig, host

Zone transfers (AXFR) provide all entries for a domain

- Used mostly for replication across secondary DNS servers

- Wealth of information, often very sensitive: subdomains, internal IP addresses and hosts, services used, ...

DNS Brute Forcing

Zone transfers are usually restricted only among authorized servers

Although misconfigurations are common...

Alternative: guess valid DNS records

Dictionary attack using A/AAAA record requests

Query based on list of commonly used subdomains, hostnames, words, etc. (e.g., www, mail, vpn, webaccess, msexchange)

DNSSEC NSEC and NSEC3 zone walking

The NSEC record is used to give negative answers to queries, but has the side effect of allowing enumeration of all names

NSEC3 mitigates this, but still allows for dictionary attacks

dnsenum <https://github.com/fwaeytens/dnsenum>

```
root@kali:~# dnsenum -f dns.txt cs.stonybrook.edu
dnsenum.pl VERSION:1.2.3
```

```
----- cs.stonybrook.edu -----
```

Host's addresses:

cs.stonybrook.edu.	5	IN	A	130.245.9.212
--------------------	---	----	---	---------------

Name Servers:

mewho.stonybrook.edu.	5	IN	A	199.110.254.244
nocnoc.stonybrook.edu.	5	IN	A	129.49.7.3
whoisthere.stonybrook.edu.	5	IN	A	129.49.7.250

Mail (MX) Servers:

aspmx2.googlemail.com.	5	IN	A	64.233.190.27
aspmx3.googlemail.com.	5	IN	A	209.85.203.27
aspmx.l.google.com.	5	IN	A	74.125.22.27
alt1.aspmx.l.google.com.	5	IN	A	64.233.190.27
alt2.aspmx.l.google.com.	5	IN	A	209.85.203.27

Trying Zone Transfers and getting Bind Versions:

Fierce <http://ha.ckers.org/fierce/>

```
root@kali:~# fierce -dns stonybrook.edu
DNS Servers for stonybrook.edu:
    mewho.stonybrook.edu
    whoisthere.stonybrook.edu
    nocnoc.stonybrook.edu

Trying zone transfer first...
    Testing mewho.stonybrook.edu
        Request timed out or transfer not allowed.
    Testing whoisthere.stonybrook.edu
        Request timed out or transfer not allowed.
    Testing nocnoc.stonybrook.edu
        Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
129.49.2.10    p250.cc.stonybrook.edu
129.49.2.6    pepprod.cc.stonybrook.edu
129.49.2.1    cisco-gw.cc.stonybrook.edu
129.49.2.2    dns4cc.cc.stonybrook.edu
129.49.2.3    peptest.cc.stonybrook.edu
129.49.2.7    psns.cc.stonybrook.edu
129.49.2.8    noldb.cc.stonybrook.edu
129.49.2.11   archive.cc.stonybrook.edu
129.49.2.12   nolpr.cc.stonybrook.edu
129.49.2.13   pepdev.cc.stonybrook.edu
129.49.2.14   twdbs.cc.stonybrook.edu
129.49.2.15   sandbox.cc.stonybrook.edu
```

Network Scanning

Identify accessible hosts, running services, service and OS versions, ...

Active: target network can observe probe requests

As opposed to passive reconnaissance or querying of public sources
Stealthiness matters! IDSes can easily detect noisy scans

Two main dimensions

Horizontal scanning: scan a subnet (or the whole internet) on a particular port number

E.g., find all hosts running a vulnerable service (internet worms)

Vertical scanning: scan all (or a subset of) ports on a given host

Scan common ports first

Manual scanning using `ping` and `netcat` can be used for quick assessments

Nmap



De facto tool for network scanning

Support for many port scan types

- sS TCP SYN scan: just wait for the ACK
- sT TCP connect scan: full connection (useful for non-root)
- sU UDP scan: protocol-specific payload for known ports
- sA ACK scan: determine if a firewall is stateful
- sO IP protocol scan: determine IP protocols (TCP, ICMP, IGMP) used
- p Specify port range (default: 1000 most common ports)

Beyond simple port scanning: extensible framework with support for third-party scripts

auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version, vuln

Service Fingerprinting

After identifying that a port is open, try to gather more information about the service

```
# nmap -sV 192.168.0.1 -p 22
```

Complete the connection and attempt to determine the software type and version

Version detection “interrogates” those ports to determine more about what is actually running

Server-initiated dialog: *banner grabbing*

Upon connection, the server transmits a banner string that often includes version information (e.g., SSH)

Client-initiated dialog: send probe application requests

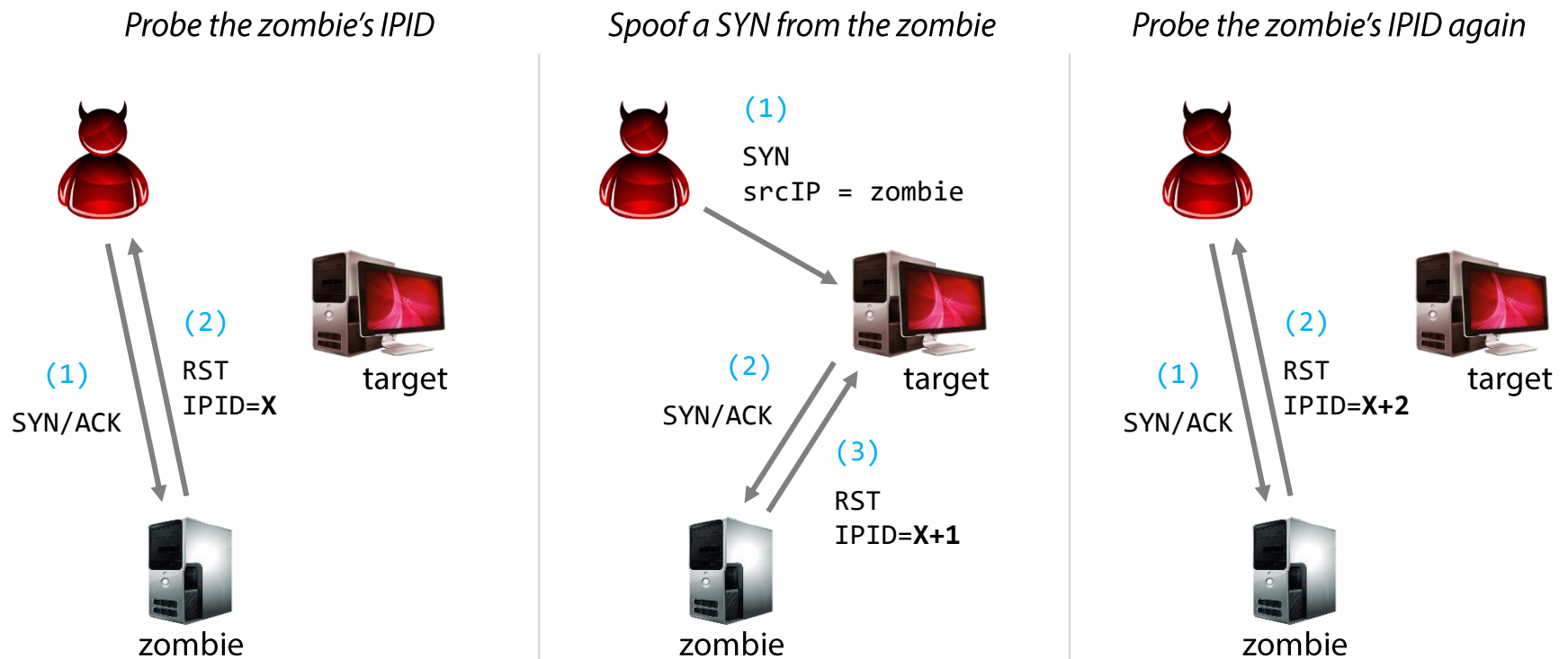
Nmap has about 6,500 dialogue patterns for more than 650 protocols such as SMTP, FTP, HTTP, etc.

Idle Scan

Hide scan attempts by blaming another “zombie” host

Zombie must be mostly idle (e.g., network printer)

Zombie should have sequential/predictable IPID behavior



ARP Scan

Useful technique for host enumeration in a LAN

Find every active IPv4 device in the same subnet

Send a “who has” broadcast packet for each IP address of interest

Example: try all 254 host IP addresses for a /24 subnet

Retry a couple of times if no response is received

Linux command-line tool: `arp-scan`

```
# arp-scan 192.168.0.0/24
```

Fast Internet-wide Scanning

<http://zmap.io>

Scan the entire IPv4 address space for a given port in ~45 minutes using a single machine and a gigabit link

Speed gains

- Eliminate per-connection state by overloading packet header fields (src port, initial Seq No.) – similar concept to SYN cookies

- Bypass TCP stack: raw socket for packet transmission, libpcap to receive responses

- Send as many probes as NIC can support

- Don't wait for timeouts – just send a fixed number of probes (usually one is enough to achieve decent coverage)

Shodan: let others do the scanning for you

Server: SQ-WEBCAM - Shodan

https://www.shodan.io/search?query=Server%3A+SQ-WEBCAM


Shodan Developers Book View All...

SHODAN Server: SQ-WEBCAM Explore Enterprise Access Contact Us

New to Shodan? Login or Register

Exploits Maps

TOP COUNTRIES



Germany	51
Lithuania	43
Hungary	37
United States	33
Poland	26

TOP SERVICES

HTTP	196
HTTP (8080)	46
HTTP (81)	25
HTTP (83)	12
HTTP (84)	6

TOP ORGANIZATIONS

TEO LT	40
Deutsche Telekom AG	40
CD-Telematika a.s.	11
Orange Polska	8
Versatel Deutschland	5

TOP PRODUCTS

Total results: 369

--- VIDEO WEB SERVER ---

88.47.208.93
c-88-47-208-93.hsd1.tn.comcast.net
Comcast Cable
Added on 2018-03-28 03:36:44 GMT
United States, Antioch
[Details](#)

HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH: 2936

61.126.182.66
p7066-1pbfx02aobadori.miyagi.ocn.ne.jp
NTT
Added on 2018-03-28 02:59:19 GMT
Japan
[Details](#)

HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH: 537

84.236.88.241
84-236-88-241.pool.digikabel.hu
DIGI Tavkozlesi es Szolgáltato Kft.
Added on 2018-03-28 01:55:29 GMT
Hungary, Eger
[Details](#)

HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH: 1002

134.255.17.171
86FF11AB.dsl.pool.telekom.hu
Magyar Telekom

HTTP/1.1 200 OK
Connection: close

Opportunistic Discovery

Use case: IPv6 address harvesting by joining pool.ntp.org

Non-published (but publicly accessible) random IPv6 addresses suddenly started getting scanned

How were they discovered?

Random guessing is ruled out: 128-bit wide addresses...

Hosts were Linux devices running an NTP daemon for time synchronization

Periodic queries to pool.ntp.org (default configuration)

Observation: IPv6 clients using brand new addresses to connect to pool.ntp.org are subsequently scanned

Probes originated from *.scan6.shodan.io hosts

The NTP servers involved were later removed from the pool

Vulnerability Scanning

Identify vulnerabilities in exposed services

Typical next step after network scanning

Exploitable bugs, misconfigurations, default passwords, ...

OpenVAS (open-source), Nessus (free/commercial, proprietary), Qualys (commercial), Nexpose (commercial), ...

New “vulnerability tests” released every day

45,000 in total for OpenVAS as of Feb. 2016

Usually come with user-friendly GUI for configuration, policy management, and report generation

Internal Reconnaissance

Directory services

X.500, LDAP, Active Directory

The “domain controller” is one of the most critical components within an organization -> holy grail for intruders

Users, privileges, endpoints, certificates, configurations, ...

SNMP (Simple Network Management Protocol)

Protocol for collecting and organizing information about network devices, and managing them

v1 basically has no authentication (cleartext “community string”)

v2 improved upon v1, but is not backwards compatible

v3 added encryption and MAC, but still not widely used

Tools: snmpenum, snmpcheck, snmpwalk, ...