Distributed Systems And Networks Coursework

Anish Katariya

(Student ID: 27561879)

Index

Contents. Page Number

A. Running the Scan

On running the penetration test on the De Militarised Zone of ECS using the Quick Scan plus mode on Zenmap there were 503 servers found to be running on the network. These servers were found using services like admdog , airport-admin , h323q931 , http , http-proxy , https , ida—agent, ida-agent , ldap , printer , sip, ssh , upnp. Most of the services found had all of their states closed. Description of the services in open states are given below.

Service	Port Number(s)	Number Of Servers	Protocol	Common Functionality
H.323/Q.931	1720	503	TCP	Used for Audio Visual Communication sessions
HTTP	80, 443, 8080	40(Found twice on some servers)	TCP	Data Communication
SSH	22	2	TCP	Secure Connection on insecure network

A.1 Open Services and ports

H.323/Q.931

On investigating the service I found that *H.323/Q.931* that runs on port 1720.It is based on 2 protocols: *H.323* and *Q.931*. *H.323* is a *VoIP(Voice over Internet Protocol)* protocol recommended by *ITU Telecommunication Standardisation Sector(ITU-T)*. It defines a protocol to provide audio-visual communication sessions on a packet network. *Q.931* is a protocol recommended by *ITU-T* for for signaling a *H.323* call. It transmits the call across networks using several protocols such as *IP, PSTN , ISDN*.

HTTP:

HTTP (*Hyper Text Transfer Protocol*)is a protocol used for data communications in the world wide web.It is managed by the *World Wide Web Consortium (W3C)*. *HTTP* functions as a request - response protocol in the client-server computing model. It is commonly used to host webpages , web apps and server application. It usually runs on ports *80 , 443* and *8080*.It uses *TCP* as a *reliable transportation protocol*.

SSh:

Ssh(Secure Shell) is a cryptographic network protocol for operating network services over unsecured networks.It provides a channel over a network in the client-server architecture , to connect an SSH Client to an SSH server. It is commonly used for remote command-line login and remote execution but any network service can be secured with SSH

B. Brief Analysis of Result

After running the test it was found that H.323/Q.931 was the most commonly run service on the network with all 503 servers running where as HTTP was running on 40 servers with 17 servers running them on two ports. HTTP was most commonly being used to run server softwares like Apache , Node.js Framework and nginx. SSH service was open on 2 ports using versions OpenSSH5.3 and OpenSSH 6.6.1. Some interesting findings interpreted from the scan are given below.

Findings and Vulnerabilities

The scan results showed several old versions of server software versions were still running on the network. Apache 2.2.15 and 2.2.22 were still commonly being used despite the current version being Apache 2.2.31 , Apache 2.4.7 and 2.4.10 were still being used despite Apache 2.4.23 being the current version and ngix versions 1.1.19 and 1.4.6 still running despite there being several security threats. I have discussed a few related to Apache 2.2.15-2.2.22 and Apache 2.4.7-2.4.10 since these softwares were being used the most

1) Apache 2.4.7 and Apache 2.4.10*(Current 2.4.23)*

- They do not have a time out mechanism, which allows remote attackers to cause a denial of service via a request to a CGI script that does not read from its stdin file descriptor.
- The log_cookie function in the mod_log_config.c in the mod_log_config module allows remote attackers to cause a denial of service(segmentation fault and deamon crash) via a crafted cookie that is not properly handled during truncation
- The dav_xml_get_cdata in the main.c/util.c in the mod_dav module in the Apache HTTP server does not properly remove white space characters from CDATA section which allows remote attackers to cause denial of service(deamon crash) via a crafted DAV script.

2) Apache 2.2.15 and Apache 2.2.22*(Current 2.2.31)*

- In these servers the mod_dav.c module does not properly determine wether DAV is enabled for a URI, which allows remote attackers to cause a denial of service(segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data which refers to a non-DAV URI
- Multiple cross-site scripting (XSS) vulnerability in the balancer_handler function in the manager interface in mod_proxy_balancer.c module allow remote attackers to inject an arbitrary web script HTML via a crafted string

C. Shortcomings of Penetration tests

Although Penetration tests have a lot of advantages to find out potential vulnerabilities in a network they should only be considered as one part of an assessment of a network's security posture as there are several vulnerabilities which may not be spotted by a penetration test however may still be enough for an attacker to exploit you network. Some of them are discussed below

1) Penetration tests are only carried on certain zones of the network and such test won't be able to detect vulnerabilities associated with local wireless access pointer attacks that could be malicious insiders currently on the internal network

2) While carrying out a penetration test there is a large possibility of crashing the target system which may cause stoppage in the normal functioning of the system.Hence some of these may not be performed during the testing phase but still might be used by attackers

3) Penetration tests can not detect if any server in the network is already infected and may be able to exploit the system.

4) Penetration test can not test for vulnerabilities associated with several attacks such as sql injection which maybe present in the source code of a particular software not within the reach of the penetration tests

5) Penetration tests if not performed properly may lead to the network accidentally leaking sensitive information.

Even though penetration tests have several advantages to and is a really helpful tool scan for vulnerabilities in a system they have to be performed carefully.There are several more tests which should be considered to fully secure the network such as vulnerability analysis.

References

1) https://wikipedia.org [Accessed 30th October 2016]
2) https://cvsdetails.com[Accessed 30th October 2016]
3) https://httpd.apache.org[Accessed 30th October 2016]