Wroclaw 6.12.2018

Secure Systems and Networks

Laboratory No. 2

Wiktor Lagiewka 219226

- **The lab room local network (e.g. 156.17.40/24 or 156.17.40.0/27) should be scanned for all services such as HTTP, HTTPS, SSH, SMTP, FTP as well as all interactive login services (telnet, rlogin, rsh and similar)**

Nmap scan report for lak.ict.pwr.wroc.pl (156.17.40.28) Host is up (0.00087s latency).

Not shown: 995 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
111/tcp open rpcbind 2 (RPC #100000)
389/tcp open ldap OpenLDAP 2.2.X - 2.3.X
2049/tcp open nfs 2-4 (RPC #100003)
3690/tcp open svnserve Subversion

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

This command will scan all of your local IP range (assuming your in the 156.17.40.28 **range), and will perform service identification (-sV)**

- **Further investigate all servers found, in order to identify versions of software running particular services.**

NSE script executed via this command: *nmap -Pn --script vuln* 156.17.40/24**.** It allows to obtain a report with found vulnerabilities. It is a list with applicable CVEs and links to exploits that exists in *Exploit Database by Offensive Security.*

- **SMTP conversation**

Available on the *dream.ict.pwr.wroc.pl/ssn* website and all the servers are closed to sending emails addressed to anybody by non-local user.

wiktor@wiktor-Lenovo-B51-80:~$ ncat -C 156.17.40.85 25
220 plonk.ict.pwr.wroc.pl ESMTP Sendmail 8.14.3/8.14.3/Debian-9.1ubuntu1+bspm1.13+rchk1.22; Thu, 15 Nov 2018 15:26:56 +0100; (No UCE/UBE) logging access from: lab21-13.technopolis.iiar.pwr.edu.pl(OK)-lab21-13.technopolis.iiar.pwr.edu.pl
[10.104.34.206]
HELO ssnmaster.pl
250 plonk.ict.pwr.wroc.pl Hello lab21-13.technopolis.iiar.pwr.edu.pl [10.104.34.206], pleased to meet you
MAIL FROM: ssn@ssnmaster.pl
250 2.1.0 ssn@ssnmaster.pl... Sender ok
RCPT TO:hpph@o2.pl
544 5.4.4 Sorry lab21-13.technopolis.iiar.pwr.edu.pl [10.104.34.206], we do not relay mail for other sites.

wiktor@wiktor-Lenovo-B51-80:~$ ncat -C 156.17.40.162 25
220 gromit ESMTP Exim 4.89 Thu, 15 Nov 2018 15:34:01 +0100
HELO ssnmaster.pl
250 gromit Hello lab21-13.technopolis.iiar.pwr.edu.pl [10.104.34.206]
MAIL FROM: ssn@ssnmaster.pl
250 OK

RCPT TO:hpph@o2.pl
550 relay not permitted

wiktor@wiktor-Lenovo-B51-80:~$ ncat -C 156.17.40.163 25
220 gromit ESMTP Exim 4.89 Thu, 15 Nov 2018 15:38:49 +0100
HELO ssnmaster.pl
250 gromit Hello lab21-13.technopolis.iiar.pwr.edu.pl [10.104.34.206]
MAIL FROM: ssn@ssnmaster.pl
250 OK
RCPT TO:hpph@o2.pl
550 relay not permitted