INFORMATION SECURITY

NMAP

Purpose

- ✓ Know how to find vulnerabilities of a system using Nmap
- ✓ Know how to find vulnerabilities/sensitive data using Google Hacking Database

Class Activities

1. Activity 1: Scan system vulnerabilities using Nmap

- Estimated Duration: 30 mins

Students download and install Nmap. Follow instructions at: http://www.youtube.com/watch?v=uNTsURvslvc to carry out 'ping sweeps', 'port scans', 'ARP poisoning', 'MAC and IP spoofing', decoys, 'OS fingerprinting'. Students try to use the following commands and try to understand them:

1. *nmap -sP 192.168.20.0/24* = Initiates ping sweep of specified network.

2. *nmap -sP -PT80 192.168.20.0/24* = TCP ping scan. Bit more sophisticated, can use port 80 (http) to traverse routers that are blocking ICMP traffic. The "-PT80" specifies port 80.

3. *nmap -sS 192.168.20.200* = Initiates a stealth port scan of the specified IP, revealing open ports and protocols.

4. *nmap -sF 192.168.20.0/24* = Port scan entire network.

5. *nmap -sF 192.168.20.0/24 -oN Scans.txt* = Port scan entire network. Save the results to a file called "Scans.txt".

6. *nmap -sS 192.168.20.200 -D 192.168.20.52* = This specifies a stealth port scan with the "-sS" option and a decoy with the "-D" option. This means we are spoofing the IP address of 192.168.20.52 while we scan 192.168.20.200. If 192.168.20.200 trusts 192.168.20.52, then it trusts us. 192.168.20.52 needs to be up and running on the net for the spoof to hides us properly, as it will be receiving SYN and ACK flag traffic.

7. *nmap -O 192.168.20.200* = Scans with the "-O" option to discover the IP protocols

8. *nmap -A 192.168.20.200* = Scan the target to discover protocols, operating system and versions. It combines –sV -O

9. *nmap -p80 -O 192.168.20.200* = Scans machine for operating system even if ports are closed using port 80 (http).

10. *nmap -h* = help (displays all the options)

- Discussion:

Students are asked to study syntax of Nmap scanner and understand the meaning of the following commands:

Nmap –sT; –sU ; –sP; -sS; -P; -v; -P0

Nmap –sS –P '1-1024' –V –P0 www.vnexperts.net

nmap –A –vv –sS –n www.vnexperts.net

nmap –vv –sU -n fit.hanu.edu.vn

2. Activitiy 2 (individual): Google hacking

- Estimated Duration: 40 mins

- Students are asked to study search keyword operators as in Appendix 1.
- Students try to use different Google keywords for gaining valuable data.
- Students are asked to hack network cameras using keywords provided in Appendix 2.
- Students are asked to find index of some websites using keywords provided in Appendix 2.
- Students are asked to find personal credentials (username/password) using keywords provided in Appendix 2
- Students are asked to find email lists using keywords provided in Appendix 2

4. References

http://dotnet.vn/ChuyenMuc/Scan-Port-toan-tap-voi-cong-cu-nmap-235.aspx

http://www.binarytides.com/google-hacking-tutorial/

http://nguoiviettre24h.blogspot.com/2013/05/huong-dan-su-dung-nmap.html

http://www.networkingprogramming.com/1024x768/linux4.html

https://www.youtube.com/watch?v=Ft5gND96EBk

Appendix 1

Keyword Operators

Lets take a look at the special google search operators that are used to construct those high powered google hack search terms.

intitle

Specifying intitle, will tell google to show only those pages that have the term in their html title. For example intitle:"login page" will show those pages which have the term "login page" in the title text.

allintitle

Similar to intitle, but looks for all the specified terms in the title.

inurl

Searches for the specified term in the url. For example inurl:"login.php".

allinurl

Same as inurl, but searches for all terms in the url.

filetype

Searches for specific file types. filetype:pdf will looks for pdf files in websites. Similarly filetype:txt looks for files with extension .txt

ext

Similar to filetype. ext:pdf finds pdf extension files.

intext

Searches the content of the page. Somewhat like a plain google search. For example intext:"index of /".

allintext

Similar to intext, but searches for all terms to be present in the text.

site

Limits the search to a specific site only. site:example.com

Link

Using this in a search will show all results that link to that url. link:www.binarytides.com returns all results that have links to www.binarytides.com.

cache

Passing cache: will return results that link to cached versions of pages Google stores. cache:brown fox will return results that contain brown and/or fox in cached pages Google's database contains.

related

When related: is used it returns results that are similar to the url you specified. Related:www.lokisec.com will return results that are similar to lokisec.com.

Appendix 2

Google hacking keywords

Hacking cameras

inurl:“viewerframe?mode=motion”
inurl:/view.shtml
inurl:"view/index.shtml"
inurl:ViewerFrame?Mode=
inurl:ViewerFrame?Mode=Refresh
allintitle:"Network Camera NetworkCamera“
inurl:"sample/LvAppl/"
inurl:"video.mjpg"
intitle:"Web Monitor" inurl:"simple.htm"
intitle:"Toshiba Network Camera" user login
Find index
allintitle:"index of/admin"
allintitle:"index of/root"
allintitle:restricted filetype:doc site:gov
allintitle:restricted filetype :mail
allintitle:sensitive filetype:doc
Find password
"Index of /" +passwd
"Index of /password"
"Index of /" +password.txt
filetype:mdb
inurl:"account|users|admin|administrators|passwd|password"
filetype:mdb inurl:users.mdb
intitle: “admin login” + inurl “admin.php” intext: “username” intext “password”
Find credential data
intitle:”curriculum vitae” “phone * * *” “address *” “e-mail:*.gov.*"
Find email list
filetype:xls inurl:”email.xls”

Other Google Hacking Keywords

allinurl:/bash_history
allinurl:winnt/system32/ (get cmd.exe)
ext:ini eudora.ini
ext:pwd inurl:(service|authors|administrators |users) "# -FrontPage-"

filetype:bak inurl:"htaccess|passwd|shadow|htusers"
filetype:conf slapd.conf
filetype:ctt "msn"

filetype:QDF QDF
filetype:pdf "Host Vulnerability Summary Report" "Assessment Report"
filetype:sql ("passwd values ****" | "password values ****" | "pass values ****")
filetype:xls inurl:"email.xls"
filetype:user eggdrop user

"Index of /admin"
"Index of /" +.htaccess
"Index of /mail"
"Index of /" "Parent Directory" "WS_FTP.ini" filetype:ini

intext:"BiTBOARD v2.0" "BiTSHiFTERS Bulletin Board"
intext:centreware inurl:status
intext:"MOBOTIX M1"
intext:"MOBOTIX M10"
intext:"Open Menu"
intext:"powered by Web Wiz Journal"
intext:"Tobias Oetiker" "traffic analysis"

intitle:index.of "Apache/1.3.28 Server at"
intitle:index.of "Apache/2.0 Server at"
intitle:index.of "Apache/* Server at"
intitle:index.of "HP Apache-based Web Server/*"
intitle:index.of "IBM _ HTTP _ Server/* * Server at"
intitle:index.of "Microsoft-IIS/4.0 Server at"
intitle:index.of "Microsoft-IIS/5.0 Server at"
intitle:index.of "Microsoft-IIS/6.0 Server at"
intitle:index.of "Microsoft-IIS/* Server at"
intitle:index.of "Netscape/* Server at"
intitle:index.of "Oracle HTTP Server/* Server at"
intitle:index.of "Red Hat Secure/*"

intitle:"Apache::Status" (inurl:server-status | inurl:status.html | inurl:apache.html)
intitle:"Welcome to IIS 4.0!"
intitle:"Welcome to Windows 2000 Internet Services"
intitle:"Welcome to Windows XP Server Internet Services"
intitle:"Welcome to Your New Home Page!"
intitle:"Test Page for Apache Installation" "It worked!" "this Web site!"
intitle:"Test Page for Apache Installation" "Seeing this instead"
intitle:"Test Page for Apache Installation" "You are free"
intitle:"Test Page for the Apache Http Server on Fedora Core"
intitle:"Test Page for the Apache Web Server on RedHat Linux"
intitle:"Test Page for the SSL/TLS-aware Apache Installation" "Hey, it worked!"

intitle:"index of" .bash_history
intitle:"index of" etc/shadow
intitle:"index.of" finances.xls
intitle:"index of" htpasswd
intitle:"Index Of" inurl:maillog
intitle:"index of" master.passwd
intitle:"index of" members OR accounts
intitle:"index.of" mystuff.xml
intitle:"index of" passwd
intitle:"index of" people.lst
intitle:"index of" pwd.db
intitle:"Index of" pwd.db
intitle:"Index of" .sh_history
intitle:"index of" spwd
intitle:"index.of" trillian.ini
intitle:"index of" user_carts OR user_cart
intitle:"active webcam page"
intitle:"ASP Stats Generator *.*" "ASP Stats Generator" "2003-2004 weppos"
intitle:"curriculum vitae" "phone * * *" "address *"
intitle:"Dell Laser Printer" ews
intitle:"EvoCam" inurl:"webcam.html"
intitle:liveapplet inurl:LvAppl
intitle:"Multimon UPS status page"
intitle:"mywebcamXP server!" inurl:":8080"
intitle:"statistics of" "advanced webstatistics"
intitle:"System Statistics" +"System and Network Information Center"
intitle:"Terminal Services Web Connection"
intitle:"Usage Statistics for" "Generated by Webalizer"
intitle:"VNC Desktop" inurl:5800
intitle:"Web Server Statistics for ****"
inurl:admin filetype:db
inurl:admin inurl:backup intitle:index.of
inurl:"auth_user_file.txt"
inurl:"/axs/ax-admin.pl" -script
inurl:"/cricket/grapher.cgi"
inurl:hp/device/this.LCDispatcher
inurl:iisadmin
inurl:indexFrame.shtml Axis
inurl:"main.php" "phpMyAdmin" "running
on" inurl:passwd filetype:txt
inurl:"printer/main.html" intext:"settings"
inurl:server-info "Apache Server Information"
inurl:"ViewerFrame?Mode="

inurl:"wvdial.conf" intext:"password"
inurl:"wwwroot/*."
inurl: “section.php?id=”
inurl: “item_id.php?id=”
inurl : “itemid.php?id=”
site:gov confidential
site:mil confidential
site:mil "top secret"
"Copyright (c) Tektronix, Inc." "printer status"
"Host Vulnerability Summary Report"
"http://*:*@www"
"Network Vulnerability Assessment Report"
"not for distribution"
"Output produced by SysWatch *"
"These statistics were produced by getstats"
"This file was generated by Nessus"
"This report was generated by WebLog"
"This summary was generated by wwwstat" "Generated by phpSystem" "Host Vulnerability Summary Report"
"my webcamXP server!"
sample/LvAppl/
"TOSHIBA Network Camera - User Login"
/home/homeJ.html