backtrack における侵入テストの実用性

杉山 仁(山梨大学 総合情報処理センタ)

sugiyama[atmark]yamanashi.ac.jp

1. はじめに

インターネットが発達し、誰もが高速な環境で気軽にWebで情報を検索した り動画を観たりと一昔前では考えられないに時代になりました。 過去では、一部のユーザーのみがインターネットサービスを利用していまし たが、現在では誰でも乗り入れるようになり、それに伴い悪意を持ったユー

ザーも増えているのが現状です。

性善説で運用されてきたネットワークも、現在では悲しいことですが性悪説 で運用することが、必然になってきました。

現在、総合情報処理センタで運用しているサーバ郡にも国内外から毎日のようにアタックが発生しています。

0	0	0		/var/log — tcsh (ttyp1)	
r=roo	ot				
Feb	9	11:07:25	localhost	sshd[29522]: Failed password for root from port 53291 ssh2	
Feb	9	11:07:33	localhost	sshd[29527]: (pam_unix) authentication failure: logname= uid=0 euid=0 ttu=ssh ruser= rhost=	se
r=roo	ot				
Feb		11:07:34	localhost	sshd[29527]: Failed password for root from port 53589 ssh2	
Feb	9	11:07:42	localhost	sshd[29529]: (pam_unix) authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost= u	se
r=roo	ot				
Feb		11:07:44	localhost	sshd[29529]: Failed password for root from the port 53931 ssh2	
Feb		11:09:01	localhost	CRON[29535]: (pam_unix) session opened for user root by (uid=0)	
Feb		11:09:01	localhost	CRON[29535]: (pam_unix) session closed for user root	
Feb		11:17:01	localhost	CRON[29565]: (pam_unix) session opened for user root by (uid=0)	
Feb		11:17:02	localhost	CRON[29565]: (pam_unix) session closed for user root	
Feb		11:33:01	localhost	CRON[29632]: (pam_unix) session opened for user nobody by (uid=0)	
Feb		11:33:01	localhost	CRON[29632]: (pam_unix) session closed for user nobody	
Feb		11:39:01	localhost	CRON[29658]: (pam_unix) session opened for user root by (uid=0)	
Feb		11:39:01	localhost	CRON[29658]: (pam_unix) session closed for user root	
Feb		12:09:01	localhost	CRON[29781]: (pam_unix) session opened for user root by (uid=0)	
Feb		12:09:01	localhost	CRON[29781]: (pam_unix) session closed for user root	
Feb		12:17:01	localhost	CRON[29811]: (pam_unix) session opened for user root by (uid=0)	
Feb	g	12:17:01	localhost	CBON[29811]: (nam unix) session closed for user root	

学内で運用しているLinuxサーバのssh アタックの形跡

特に、組織で運営しているネットワークですので、踏み台にされて、そこか ら別のネットワークへの攻撃の拠点にされてしまいますと、組織としての信 用が失われます。

今では、どこの組織もfirewallを導入して必要なサービスをしているサーバ や使用しているサービスポート以外は、外部との接続は遮断していると思い ますが、今までの外部攻撃がfirewallによって効かなくなった分、内部から の攻撃にシフトしているとの調査結果もあります。(※1)

そこで、攻撃に対し耐えられるシステム構築をしているか、侵入テストの分 野に設計・開発されたLinuxディストリビューションであるbacktrackを使用 して安全確認する方法を報告いたします。

Debian,OpenSUSE,FreeBSD等のPC-UNIXが稼働するPCで各種ツールをインストー ルすれば済むと考えるかも知れませんが、backtrackのCDまたはUSBを持ってさえい れば、どこでもテスト可能であることと、各種ツールのインストール作業が必要ない のは大変魅力的です。

### 2. backtrackとは

侵入テストの分野に設計・開発されたLinuxディストリビューションであり、 侵入や攻撃のツール群が予めインストールされています。

公式サイト(※2)より、ライブCD版とUSBドライブ版、VMware版の3種類が ダウンロード可能です。

USB版・Vmware版の使用が、使い勝手が良いと思います。それはOSの設定 変更が反映されるからです。ライブCDでの使用は、変更した設定等を保存 する領域がありません。ただ、USB版はUSBへのインストールする為のもの ですが、インストールが多少苦労するかも知れません。使用するにあたりも っとも簡単なのは、ライブCD版又はVMware版の使用です。今回は、VMware 版を使用しています。



起動したbacktrack3 既にツール類がインストールされている。 ディスクトップ環境はKDE

#### 3. 調査の流れ

backtrackに各種ツールがあっても、調査するにあたり適当にツールを使用 しても効率的ではありません。

ここは、クラッカーの立場として考えて見ることが必要です。

3.1 情報の収集

ターゲットとなるホストや、該当するネットワークを決めます。

webでの検索、nslookup,whoisコマンド等で調査を行います。

特にNetcraft(※3)のサイトは、非常に便利です。

3.2 スキャニング

調査対象のホストに対し、そのホストがどのような**OS**でどのようなサービス を行っているのかを調査します。**OS**や提供しているサービスがわかれば攻撃 手段が絞れてくるからです。

サービスは、開いているポートを発見したら、telnetコマンド等でサービス バナー情報を取得すれば、さらに詳細がつかめます。防御側としてはバナー を表示しない、もしくは偽りの情報を表示するように設定を変更するとよい でしょう。

3.3 侵入

調査対象のホストのOS・サービスのバージョンをスキャニングで調査した後、 そのホストの脆弱性をつくExploitを仕掛けます。リモートログイン可能な状 態(FTP,Telnet,ssh等のサービスが稼働)の場合は、ソフトの初期設定で使用 しているユーザー名・パスワードや、ホスト名や組織の名称、組織のwebか ら得た情報(メールアドレス等)から予測したユーザー名とパスワード、そし てパスワード辞書を使用した総当たり攻撃も有効です。

侵入に成功した場合、そのユーザーから管理者権限のあるユーザー (root,administratorなど)へスイッチする場合もExploitを使用します。

管理者権限さえ取得出来れば、そのホストは自分のものになったようなもの です。バックドアを仕掛けたり、そのホストを踏み台にして他のホストへの 接続をしたり(組織内の接続は甘い場合も多い)、自分のファイル置き場でも 自由に使用出来ます。 3.4 証拠隠滅

侵入したホストで作業をすれば、その作業内容がそのままlogとして保存されます。logから侵入されたことが判明すれば、そのホストは二度と使えません。そこで侵入した形跡を消去します。該当のlogを消去するツールもネット上で公開されています。

防御側としては、例え改竄されたlogでも侵入と判断出来る場合もあります。ある時間帯だけlogが不自然である、log自体のファイルサイズがO(/dev/nullへのシンボクリックリンク)など、証拠を削除されても何かしら違和感があります。注意深くlogを確認することが大切です。

- 4. ツールの使用
  - 4.1 攻撃の第一歩

まずは、攻撃対象のサーバがどのようなサービスを提供しているか調べます。 サービスを調査するのには、ポートスキャンを行います。

Nmap(※4)は、Windowsでも稼働する最もポピュラーなツールです。あらゆ るOS用のbinaryやソースコードが公開されているので、特にbacktrackだか ら楽に使えるというものではありません。

Nmapは、KDEメニューから"Backtrack→Network Mapping→All→Nmap" にあります。

ネットワーク上にサービスポートの開いているホストを探す場合は、以下のコマンドオプションでスキャンします。

nmap -v -sP 192.168.10.0/24

**IP**アドレスの第三オクテットまでが**192.168.10.**\*のネットワーク上に存在 するホストをスキャンしています。

6	Shell - Nmap	
Host	192.168.10.145 appears to be up.	
Host	192.168.10.146 appears to be up.	
Host	192.168.10.147 appears to be up.	
Host	192.168.10.148 appears to be up.	
Host	192.168.10.149 appears to be up.	
Host	192.168.10.150 appears to be up.	
Host	192.168.10.151 appears to be up.	
Host	192.168.10.152 appears to be up.	
Host	192.168.10.153 appears to be up.	
Host	192.168.10.154 appears to be up.	
Host	192.168.10.155 appears to be up.	
Host	192.168.10.156 appears to be up.	
Host	192.168.10.157 appears to be up.	
HOST	192.168.10.158 appears to be up.	
HOST	seriousbarbarian. (an (192.108.10.159) appears to be up.	
Host	192,168,10,160 appears to be up.	
lloct		
Host	192 169 10 163 appears to be up	
Host	192 166 10 164 appears to be up	
Host	192 166 10 165 appears to be up	
Host	192.168.10.166 appears to be up.	
Host	192,168,10,167 appears to be up.	
Host	192.168.10.168 appears to be up.	555
Host	192.168.10.169 appears to be up.	222
Host	192.168.10.170 appears to be up.	
Host	192.168.10.171 appears to be up.	
Host	192.168.10.172 appears to be up.	
Host	192.168.10.173 appears to be up.	
Host	192.168.10.174 appears to be up.	
Host	192.168.10.175 appears to be up.	
Host	192.168.10.176 appears to be up.	
Host	192.168.10.177 appears to be up.	
Host	192.168.10.178 appears to be up.	
and the second value of th		

実行した結果、192.168.10.159にホストがありました。 発見したホストに対して、再度以下のコマンドオプションで実行してみます。

nmap -v -A -O 192.168.10.159

下記は、nmap実行結果を一部抜粋したものです。



この結果により、該当のIPはsshdが稼働しているMac OSXのホストだと判明

します。

このように、簡単に稼働しているホストや、そのホストが提供しているサービスが簡単にわかります。

# 4.2 Metasploit Framework

攻撃対象のホストのOSがわかれば、そのOSにあわせた攻撃が出来ます。 Packet Storm(※5)等のサイトからツールをダウンロードしインストールするのは 大変面倒な作業です。

backtarckには、Metasploit Framework(※6)という強力なExploitツールがあり ます。

KDEメニューから"Backtrack→Penetration→Framework Version3"に関連 のツール群があります。

まずは、"Framework3-MsfUpdate"を実行します。

実行後、Metasploit Frameworkは最新状態になります。そして"Framework3-MsfGUI"を実行します。



Metasploit Framework 起動画面(某ゲームを真似ています③)

🖉 💿 Metasploit Framework GUI v3.3-dev		8				
<u>S</u> ystem <u>W</u> indow <u>H</u> elp						
🗙 Cancel 💽 Fir	nd	Jobs				
		Job ID Module				
		Jobs				
Kernel Exploits     All loaded exploit modules (288)						
bsdi						
Freebsd						
hpux						
P 🖬 multi						
In netware						
Solaris						
P test						
	JUL	(Benelow)				
Module Information Module Output		Sessions				
Module: exploit/inux/imap/imap_uw_jubb         This module exploits a buffer overflow in the 'LSUB' command of the University of Washington IMAP service. This vulnerability can only be exploited with a valid username and password. This exploit module was written by patrick (patrick@aushack.com)         References:         http://www.secutifycous.com/bid/1110         http://www.secutifycous.com/bid/1110         http://www.milw0mm.com/exploits/284						
Loaded 288 exploits, 124 payloads, 17 encoders, 6 nops, and 56 auxiliary						

#### Metasploit Framework メイン画面

画面を見ると、Expolits(OSの脆弱性を利用するツール),Auxiliary(攻撃 ツール),OSごとに分類されています。項目をクリックすることにより、 簡単に利用出来ます。

今回、時間の関係で検証用のサーバ(古いOSやパッチの当たってないOS) が用意出来なかったため脆弱性確認することは出来ませんでしたが、 OSXのsambaへの攻撃例を示します。

この脆弱性はOSX 10.4.Xの脆弱性です。今回の攻撃対象はOSX 10.4.Xですが、 既にパッチ対応済みの為、失敗に終わります。

http://support.apple.com/kb/HT1457?viewlocale=ja\_JP

System Windw Help     Image: Same Same Same Same Same Same Same Same	🗰 💿 Metasploit Framework GUI v3.3-dev	1		
▶ arb   ▶ browser   ▶ arb   ▶ browser   ▶ arb   ▶ arba   ★ transZopen   Samba   ★ transZopen   Samba transZopen Overflow (Mac OS X)   ▶ arbs   ★ test   ▶ arbs   ★ test   ▶ arbs   ▶ arbs <td< th=""><th><u>S</u>ystem <u>W</u>indow <u>H</u>elp</th><th></th><th></th><th></th></td<>	<u>S</u> ystem <u>W</u> indow <u>H</u> elp			
P Inctware   P oxx		<u>Find</u>	lob ID Module	
O osx/samba/trans2open     osx/samba/t	P netware		⊽ 💂 Jobs	
I a rip I a	V 🖻 05X		0 osx/samba/trans2open	
A skela A skela A smile A mile B orwser B email B mail B ftp This matures theap Samba isa jo trans names Heap Overflow This matures theap Samba isa jo trans names Heap Overflow This matures theap Samba isa jo trans names Heap Overflow This mature transcopen Samba transcopen Overflow (Mac OS X) P a solaris B est Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris D test Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris D test Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris D test Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris D test Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris D test Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris D test Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris P a solaris Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris P a solaris Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris P a solaris P a solaris Notule transcopen Samba transcopen Overflow (Mac OS X) P a solaris Notule transcopen Samba transcopen Overflow induce was written by Ramodified transcopen Samba t	🕨 🛅 afp			
A armie A armie B browser A armie B browser A armie B browser A armie B armie	🕨 🖻 arkeia			
b browser     b canal     b canal     b canal	👂 🛅 armie			
In the state of	b browser			
Intervence: Network: 124 bavloads. 17 encoders, 6 nots, and 56 auxiliary	👂 🛅 email			
samba   Image: Sa	▶ 🖻 ftp			
Sandard 288 exploits. 124 pavloads. 17 encoders, 6 nops, and 56 auxiliary	🗢 🛅 samba			
	👹 Isa_transnames_heap Samba Isa_io_trans_names Heap Overflow			
Isolaris Itest Module Information Module Output Module: exploit/osx/samba/isa_transnames_heap This module triggers a heap overflow in the LSA RPC service of the Samba daemon. This module uses the szone free () to overvite receip pointer in initial malioc, zones structure. This exploit module was written by Ramon de Carvaho Valle (ramon@risesecurityorg) and Adriano Qrisesecurityorg) and hdm (ndm@metasploit.com) References: http://cve.mitre.org/col-bin/cvename.cqi?name=2007-2446 Loaded 288 exploits. 124 pavloads. 17 encoders, 6 nops, and 56 auxiliary	👹 trans2open Samba trans2open Overflow (Mac OS X)			
Control of the step of the step of the second of the same sheap      This module triggers a heap overflow in the LSA BPC service of the Samba daemon. This module uses the szone free     to overwrite the size() of ref() pointer in thild. malloc zones structure. This exploit module was written by Ramon     de Carvaho Valle (ramon@risesecurityorg) and Adriano Lima (adriano@risesecurityorg) and hdm     (hdm@metasploit.com)  References:     http://cve.mitre.org/cgl-bin/cvename.cgl?name=2007-2446	Isolaris			
Notice Information       Module Output         Module: exploit/josx/samba/sa_transnames_heap         This module triggers a heap overflow in the LSA RPC service of the Samba daemon. This module uses the szone_free () to overwrite the size() or free() pointer in initial_malloc_zones structure. This exploit module was written by Ramon (hdm@metasploit.com)         References:         http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-2446	test			
Module: exploit/osx/samba/isa_transames_heap         This module triggers a heap overflow in the LSARPC service of the Samba daemon. This module uses the szone_free () to overwrite the size() or free() pointer in initial malloc_zones structure. This exploit module was written by Ramon (hdm@metasploit.com)         References: http://cve.mitre.org/cgi.bin/cvename.cgi?name=2007-2446	Nodule Information Medule Output		Sessions	
This module triggers a heap verflow in the LSA PPC service of the Samba daemon. This module uses the szone free () to overwrite the size() or free() pointer in initial mailoc zones structure. This exploit module was written by Ramon de Carvaho Valle (ramon@risesecurityorg) and Adriano Eima (adriano@risesecurityorg) and hdm (hdm@metasploit.com) References: http://cve.mitre.org/cgi.bin/cvename.cgi?name=2007-2446	Module: exploit/osy/samba/isa transnames bean		Target Type	
Laded 288 exploits. 124 payloads. 17 encoders, 6 nops, and 56 auxiliary	This module triggers a heap overflow in the LSA RPC service of the Samba daemon. This module uses the szc () to overwrite the size() or free() pointer in initial malloc zones structure. This exploit module was written by de Carvalho Valle (ramon@risesecurityorg) and Adriano Lima (adriano@risesecurityorg) and hdm (hdm@metasploit.com) <b>References:</b> http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-2445	one_free Ramon		
	Loaded 288 exploits, 124 payloads, 17 encoders, 6 nops, and 56 auxiliary	][		

画面の"Expolits→osx→samba→lsa\_transnames\_heap"をダブルク リックで選択します。

# 0	Samba Isa_io_trans_names Heap_Overflow	
	:::RSSiStant	
Select your target		
Select your payload		
Select your options	Mac OS X 10.4.x x86 Samba 3.0.10	-
Confirm settings		
<u>S</u> ave		
	Sancel	vard

攻撃対象のOSとサービスのバージョンが表示されます。 "Forward"ボタンを押下します。

# 0	Samba Isa_io_trans_names Heap_Overflow 📃 🕅
# 115	ASSISTANT
<u>H</u>	
Select your target	generic/shell_reverse_tcp
Select your payload	
Select your options	
Confirm collings	Connect back to attacker and spawn a command shell
Commisseungs	
Save	
	Sancel

攻撃対象のホストのshellが使用出来るオプションを選択し、"Forward" ボタンを押下します。

# 0	Samba Isa_io_trans_names Heap Overflow <2>	
#	MSF:: ASSiStant	
Select your target	Samba Isa_io_trans_names Heap Overflow	
Select your payload	👻 Standard	
Select your options		
Confirm settings	RHOST : The target address	_
Commisseurigs	[192.168.10.159]	
Course of the second se	PPOPT - Set the SMB service nort	
□ ⊇ave	445	
	SMBPIPE : The pipe name to use	
	LSARPC	
	LPORT : The local port	
	4444	
	LHOST . The local address	
	192.168.75.128	
	▶ Advanced	
	💥 Cancel 😂 Back 🖨 Fo	rward

攻撃対象のIPアドレスを入力し、"Forward"ボタンを押下します。



設定を確認し、"Apply" ボタンを押下すると攻撃が始まります。

🗰 🔟 Metasploit Framework GUI v3.3-de	v					
System Window Help						
Cancel	Find	Jobs				
		Job ID	Module			
🕑 💼 netware		v 🖵 Jobs	5			
🗢 🛅 osx		0	) osx/samba/trans2open			
👂 🛅 afp						
🕨 🛅 arkeia						
The armie						
b browser						
🕨 🖿 email						
D 🖻 ftp						
V 🖻 samba						
Wisa_transnames_heap_Samba isa_io_trans_names Heap Overflow						
w trans2open Samba trans2open Overflow (Mac OS X)						
P isolaris						
Module Information Module Output		Sessions				
Module: exploit/osx/samba/lsa_transnames_heap		Targ	et Type			
Module:       exploit/os/samba/isa_transnames_heap         This module triggers a heap overflow in the LSA PC service of the Samba daemon. This module uses the szone free () to overvite the size() or free() pointer in initial malloc_zones structure. This exploit module was written by Ramon de Carvalho Valle (ramon@risesecurityorg) and Adriano Lima (adriano@risesecurityorg) and hdm (hdm@metasploit.com)         References:       http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-2445         http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-2445						
Loaded 288 exploits, 124 payloads, 17 encoders, 6 nops, and 56 auxiliary						

右上のjobが実行中の攻撃

攻撃に成功すると、右下のSessionに攻撃したホストが表示されshellが 実行可能になります。

今回は、失敗したため、右上のjobの表示が無くなるだけでした。

### 4.3 Hydra

Nmapで調査した結果OSXのホストにsshdが動いていました。そこでsshで、 そのホストに接続してみたいと思います。

総合情報処理センタで運用しているサーバ郡にも国内外から毎日のようにsshアタッ クが発生しています。IDとパスワードの辞書ファイルを使用し、コンピュータに疎い ユーザーのIDとパスワードを総当たりで探す手段です。

もちろん、そのツールもインストールされています。

KDEメニューから"Backtrack→Privilege Escalation→PasswordAttacks→ PasswordOnlineAttacks"に関連のツール群があります。

メジャーなHydraのGUI版であるXHydra(※7)を試してみます。

🖹 🗐 HydraGTK 📃 🚍 🕅						
🛃 Quit						
Target Passwords Tuning Specific	c Start					
Target						
Single Target	127.0.0.1					
Target List	/root/Desktop/ip.list					
Port	22					
Protocol	ssh2					
1 Interest	33112					
-Output Options						
IIce SSI	Be Verbose					
USE SE	be verbose					
Show Attempts	Debug					
hydra -M /root/Desktop/ip.list ssh2 -s 22 -L /root/Desktop/user.list -P /root //						

XHydraのターゲット設定画面

総当たりアタックする攻撃対象のIP(またはホスト名),サービスポート, プロトコルを設定します。

テキストファイルを作成し、リストを作っておけば複数のホストに対して自動的にアタックを行います。

🕱 💿 HydraGTK 📃 🖃 🕱							
Nuit Quit							
Target	Passwords	Tuning Specific	Start				
Userna	me						
	🔵 Userna	ame	yourname				
	🖲 Useman	ne List	/root/Desktop/user.list				
Passwo	rd						
	Passw	vord	yourpass				
	Passwork	rd List	/root/Desktop/pass.list				
Colon s	eperated file	e					
Use Colon seperated file							
Try login as password Try empty password							
hydra -M /root/Desktop/ip.list ssh2 -s 22 -L /root/Desktop/user.list -P /root  //							

ユーザーIDとパスワードの設定画面

ホストに登録されているであろうユーザーIDとパスワードを設定しま す。テキストファイルを作成し、ユーザーIDとパスワードのリストを作 っておけば複数のホストに対して自動的にアタックを行います。

インターネット上には、よく使われるユーザーIDやパスワードのリストが公開されています。(辞書ファイル)それらを利用することもおすすめします。



スタート画面

設定が終われば、後は"Start"ボタンを押下すれば実行します。



実行結果

sshアタックに成功すると、太文字で接続が成功したIP(ホスト名)とIDと パスワードが表示されます。

後は、判明したIDとパスワードで手動で接続して下さい。

5. まとめ

今回紹介したツール以外にも様々なツールがインストールされています。 (例えばCISCO出荷時のデフォルトのパスワードがある機器を検索するツールや、無線LAN のWEPキー解析ツールなど)

全て紹介すると一冊の本になるでしょう。どこかの出版社で出版して頂くと ありがたいですが。

今回はbacktrackの紹介というよりは、インストール済みのツールの紹介で すが、これらのツールがインストール不要で使用出来るのは、大変魅力的で す。新規にサーバを立ち上げた時や、許可なくサービスをしているサーバを 探し、そのサーバが正しく運用されているかの調査など大変実用的なディス トリビューションです。

(もちろん、使用するにあたり調査対象のホスト管理者やネットワーク管理者に許可を取ら なくてはいけません。) 専用のPCを持たなくてもライブCDやUSBで、どのPCでも調査用のPCになる こともかなり実用的だと思います。

是非、この**backtrack**を使用して組織内の安全を保つのに役立ければと思います。

## 謝辞

山梨大学総合情報処理センタの佐藤様には、このような報告書を書く機会を頂 き、ここに深く感謝いたします。 参考web

- ※1 金融機関のシステム攻撃は外部よりも内部から(ITmediaエンタープライズ2005年6月23日)
   http://www.itmedia.co.jp/enterprise/articles/0506/23/news007.html
- ※2 backtrack公式web http://www.remote-exploit.org/backtrack.html 現在(2009/02/28)Version4のβ版が、ubuntuベースとなって公開されている。
- %3 netcraft http://news.netcraft.com/
- %4 Insecure.Org Nmap Free Security Scanner, Tools & Hacking resources http://insecure.org/
- %5 [packet storm] http://packetstormsecurity.org/
- %6 The Metasploit Project http://www.metasploit.com/
- ※7 Hydra公式web http://freeworld.thc.org/

参考書籍

O'REILLY Andrew Lockhart著 ネットワークセキュリティHacks 第2版 ISBN 978-4-87311-327-2