Security testing with nUbuntu

TESTY EFT

visuellewerkstatt.de, photocase.com

Study your network's defenses with the Ubuntu-based nUbuntu security testing distribution. **BY RUSS MCREE**

Several Linux distros address the needs of the information security professional. If you've had any exposure to the tools of the trade [1], you've probably heard of distributions such as BackTrack, Helix, KcPentrix, or Knoppix-STD. An Ubuntu-based security distro is also available. nUbuntu (network Ubuntu) is best described as Ubuntu for the security aware. According to the nUbuntu website, the goal of the nUbuntu project is "… to create a distribution that is derived from the Ubuntu distribution, add packages related to security testing, and remove unneeded packages, such as Gnome, Openoffice.org, and Evolution." In other words, nUbuntu goes light on the GUI desktop but comes with a long list of security tools for scanning, enumeration, fuzzing, attacking passwords, sniffing, and spoofing.

The current version of nUbuntu is based on Ubuntu 6.10 "Edgy Eft." Like the other Ubuntu derivatives, nUbuntu is all Ubuntu underneath. Because the main attraction with this Linux is the security tools – no one is going to install nUbuntu as an end-user system – I decided to focus on nUbuntu's security utilities. In this article, I introduce a few of the useful and interesting security applications you'll find in nUbuntu. Of course, common testing tools such as Nmap, Yersinia, Ettercap, Kismet, Dsniff, and Wireshark are also available, but because these tools are already well documented, I'll focus on utilities that are useful but less well known. A summary of additional nUbuntu security tools is shown in Table 1.

Getting Started

The vast majority of the scripts included in nUbuntu run best from their individual directories rather than from the menu. Open a terminal and *cd* to */tools*, then enter *ls* to list the contents of the */tools*directory. Directories for the major tool categories and subdirectories for the various tools are found in each category. Some tools, such as Amap, Nmap, and Wireshark, run right from */usr/bin*.

BED v0.5

BED, or the Bruteforce Exploit Detector [2], is a rudimentary but useful fuzzer. Fuzzing is an excellent way to find flaws in network applications, basically by

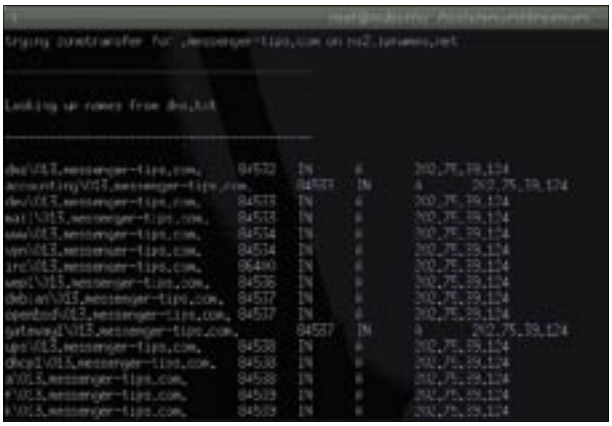

Figure 1: Spot the SPIMmer with DNS Enum.

breaking them. Thus, if I fuzz a web server on port 80 and it fails, it could well be vulnerable. Creator Martin Muench describes BED v0.5 as "… a collection of scripts to automatically test implementations of different protocols for buffer overflows and/or format string vulnerabilities, by sending a lot of long strings to a server in a boring, stupid way" [3]. He's a little hard on himself, in that the tool does its job well. If you change to the */tools/fuzzers/bed* directory, you can then run *./bed.pl* for usage feedback. For a quick test, I fired up an older Knoppix release in a secondary machine and set BED loose against httpd over port 80:

```
./bed.pl -s HTTP -t ➥
192.168.238.53
```

The *-s* option calls your plugin of choice (such as ftp, http, SMTP, POP, IRC, or LPD), and *-t* indicates the target.

If http is running on a different port, you can add the *-p* option. You might have to wait a while before BED finishes a complete cycle. Listing 1 is an example of BED output.

If httpd crashes, you know you've found a soft spot. For more information on fuzzing, see "Stack Overflow Exploitation Explained" [4].

DNS Enum

For testing your name resolution system, nUbuntu includes an efficient little script called DNS Enum that enumerates DNS information. To use DNS Enum in nUbuntu, first go to */tools/enum/dnsenum*, then enter:

```
perl dnsenum.pl domain_name ➥
dns.txt
```

A well-managed domain won't give up too much information or a zone transfer. Enumerating a domain like *sans.org* shows only the name servers, failed zone transfer attempts, no C class IPs returned, no responses to reverse lookups, and no responses to the queries listed in *dns.txt*. However, at the opposite extreme, a query of a pseudo-malicious site like *messenger-tips.com* (don't go there) results in a response for every query in *dns.txt* (Figure 1). That's so that when you're *spimmed* (spammed in IM) with a random URL, (i.e., **.messenger-tips.com*), you'll receive the root URL regardless – effective for social engineering and annoying in every way.

Listing 1: BED Output

```
01 BED 0.5 by mjm ( www.codito.de ) & eric ( www.snake-basket.de )
02
03  + Buffer overflow testing:
04                testing: 1      HEAD XAXAX HTTP/1.0     ..........
05                testing: 2      HEAD / XAXAX    ..........
06                testing: 3      GET XAXAX HTTP/1.0      ..........
07                testing: 4      GET / XAXAX     ..........
08                testing: 5      POST XAXAX HTTP/1.0     ..........
09                testing: 6      POST / XAXAX    ..........
10                testing: 7      GET /XAXAX      ..........
11                testing: 8      POST /XAXAX     ..........
12  + Formatstring testing:
13                testing: 1      HEAD XAXAX HTTP/1.0     .......
14                testing: 2      HEAD / XAXAX    .......
15                testing: 3      GET XAXAX HTTP/1.0      .......
16                testing: 4      GET / XAXAX     .......
17                testing: 5      POST XAXAX HTTP/1.0     .......
18                testing: 6      POST / XAXAX    .......
19                testing: 7      GET /XAXAX      .......
20                testing: 8      POST /XAXAX     .......
```

Driftnet

I find Driftnet highly entertaining, and you may as well, so long as you are absolutely clear on its purpose. According to the project homepage [5], Driftnet "… listens to network traffic and picks out images from TCP streams it observes." Chris Lightfoot, the developer, sums it up best: "Obviously, Driftnet is an invasion of privacy of a fairly blatant sort. Also, if you are possessed of Victorian sensibilities and share an unswitched network with others who are not, you should probably not use it."

Pseudo-legalese aside, Driftnet is a useful tool for monitoring violations of your acceptable use policy (Figure 2). Just remember, when monitoring a corporate network, it is essential to display a logon banner indicating to users that they are subject to monitoring and potential disciplinary action if violations are noted.

The violations you are likely to note with this tool will likely include poten-

Table 1: Other nUbuntu Security Tools

Tool	Description
Metasploit	An open source platform for developing, testing, and using exploit code.
Nmap	The de facto standard port scanner.
Yersinia	A network tool designed to take advantage of weaknesses in network protocols.
Ettercap	A multipurpose sniffer/interceptor/logger for switched LANs.
Kismet	An 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system.
Wireshark	A network protocol analyzer, formerly Ethereal.
GooScan	A tool that automates queries against Google, designed to find potential vulnerabilities on web pages (violates Google's Terms of Service).
MD5coll	An MD5 collision generator.
RainbowCrack	Hash cracker that uses the faster time-memory trade-off technique.
Amap	A tool for performing fast, reliable application protocol detection independent of the TCP/UDP port.
Dsniff	Packet sniffer and traffic analysis tools that decode information sent across the network, rather than simply capturing and printing raw data.

Figure 2: Monitoring images sent over your network with Driftnet.

tially disturbing images, so be prepared. I like to run Driftnet as follows:

```
/usr/bin/driftnet -v -I eth0.
```

This command will also dump rudimentary network activity to the terminal, like a simplified Tcpdump. Images can be saved to the current directory by clicking on them in the resulting viewer window. After booting nUbuntu, you can also install the tiny screenshot utility Scrot. Type

```
sudo apt-get install scrot
```

at a terminal prompt, then issue *scrot -s imagename.png* > , where *imagename* is a name you choose, and select the screen area you want to capture.

As an added bonus, Driftnet can also capture MPEG audio. Also, you can configure it to run in adjunct mode so that other programs can gather images from the network.

PBNJ 2.04

PBNJ [6] is worthy of its own article (Figure 3). PBNJ is a "… suite of tools to monitor changes on a network over time. It does this by checking for changes on the target machine(s), which includes the details about the services running on them as well as the service state." You might be familiar with Nmap

Listing 2: Extracting URLS with List-URLs

```
01 ################################
02 #                              #
03 #          Extract URLS from a web page #
04 #             muts@whitehat.co.il #
05 #                              #
06 ################################
07
08 http://www.pnwer.org/portal/psacs
09 http://www.cyberconflict.org/
10 http://stopbadware.org/
11 http://bleedingsnort.com/
12 http://www.owasp.org/index.jsp
13 index.htm
14 contact.htm
15 toolsmith.htm
16 howtos.htm
17 simplicity.htm
18 standards.htm
19 practices.htm
20 philosophy.htm
21 publications.htm
22 links.htm
23 definition.htm
24 gnugpl.htm
25 http://holisticinfosec.blogspot.com/
26 http://validator.w3.org/check/referer
27 http://jigsaw.w3.org/css-validator/
28 sec_dash/index.htm
29 http://labs.idefense.com/software/malcode.php
30 http://www.cisecurity.org/
31 http://issa.org
32 toolsmith.htm
33 http://www.owasp.org/images/0/01/Secure_Web_App_Server_McRee_OWASP.pdf
```

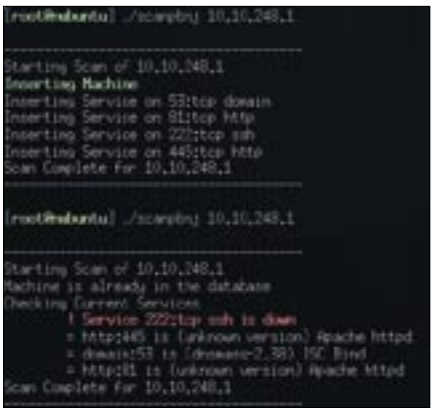

Figure 3: Monitoring changes with PBNJ.

[7], the time-honored port scanner. PBNJ will parse the data from a scan, store it in a database, and use Nmap to perform scans. Database options include SQLite (default), MySQL, Postgres, and CSV. The two primary components of PBNJ are *scanpbj* and *outputpbnj*. Scanpbnj will use Nmap to conduct the actual scan, and Outputpbnj will format the results. If you like, you can choose to schedule scans via cron jobs.

To test the value of PBNJ, go to */tools/scanners/pbnj-2.04 directory* and enter:

```
./scanpbnj IP_or_hostname
```

For the next example, I scanned an IPCop firewall with SSH enabled then disabled, indicating how a small tool like PBNJ could serve as a network tripwire, monitoring critical systems for changes at regular intervals. To generate a CSV report, execute:

```
./outputpbnj -q latestinfo ➥
-t csv Report.txt.
```

INFO

[1] Security distros: *http://www.securitydistro.com*

[2] BED: *http://www.cobra-basket.de/bed.html*

[3] nUbuntu: *http://www.nubuntu.org/about.php*

[4] "Stack Overflow Exploitation Explained": *http://milw0rm.com/papers/140*

[5] Driftnet: *http://ex-parrot.com/~chris/driftnet/*

[6] PBNJ: *http://pbnj.sourceforge.net/*

[7] Insecure.org: *http://www.insecure.org*

[8] Badstore: *http://www.badstore.net*

[9] Foundstone: *http://www.foundstone.com/us/index.asp*

Figure 4: ISR-Form pulls information from HTML tags.

nUbuntu also comes with a couple of little scripts that are useful for reconnaissance against a website you've been asked to include in your enterprise penetration test.

WWW Enumeration

ISR-Form is a simple HTML parser that pulls information from HTML *form* tags to analyze web applications (Figure 4). To use ISR-Form, enter:

```
wget -r www.yoursite.com
```

to recursively download a site you want to analyze. Change to */tools/enum/isr-form-1.0* then enter:

```
./isr-form.pl -l ➥
/home/nubuntu/ ➥
www.yoursite.com ➥
-o /home/nubuntu/ ➥
www.yoursite.com. ➥
form.txt.
```

This command will send all form tag findings to a report file that you can use to validate input methodology in the page code.

Another web-related script in nUbuntu is List-URLs, which extracts all URLs from a page (Listing 2). To run List-URLs, change to */tools/enum/list-urls* and enter:

```
./list-urls.py ➥
http://yoursite.com.
```

This script offers a quick, easy way to learn a good deal about a site and its relationships with other sites.

Summary

Enhanced security is a function of increased awareness, and security distros like nUbuntu can help heighten your awareness of potential threats. Security practitioners, and the merely curious, will find nUbuntu a useful and educational distribution, but, as with all security-oriented tools, you can get yourself in a good deal of trouble should you test against systems that aren't yours.

This distro, and the applications it includes, are designed to uncover vulnerabilities; the tools I describe can quite easily bring a server to its knees. Let common sense prevail, and you'll find yourself with hours of useful discovery.

I recommend a local LAN, unique to you, with a small switch and a virtual machine host where you can mount images of vulnerable systems from Badstore.net [8] or Foundstone [9] that you can practice on.

nUbuntu is a fairly young project that is looking for additional support. If you want contribute, contact Tom Bell at tomb@nubuntu.org. ■