BACKBOX LINUX & METASPLOIT

@AndreaDraghetti

Open Source Day - 28 Novembre 2015

About Me

BackBox Team Member

Over Security Founder

Independent Security Researcher

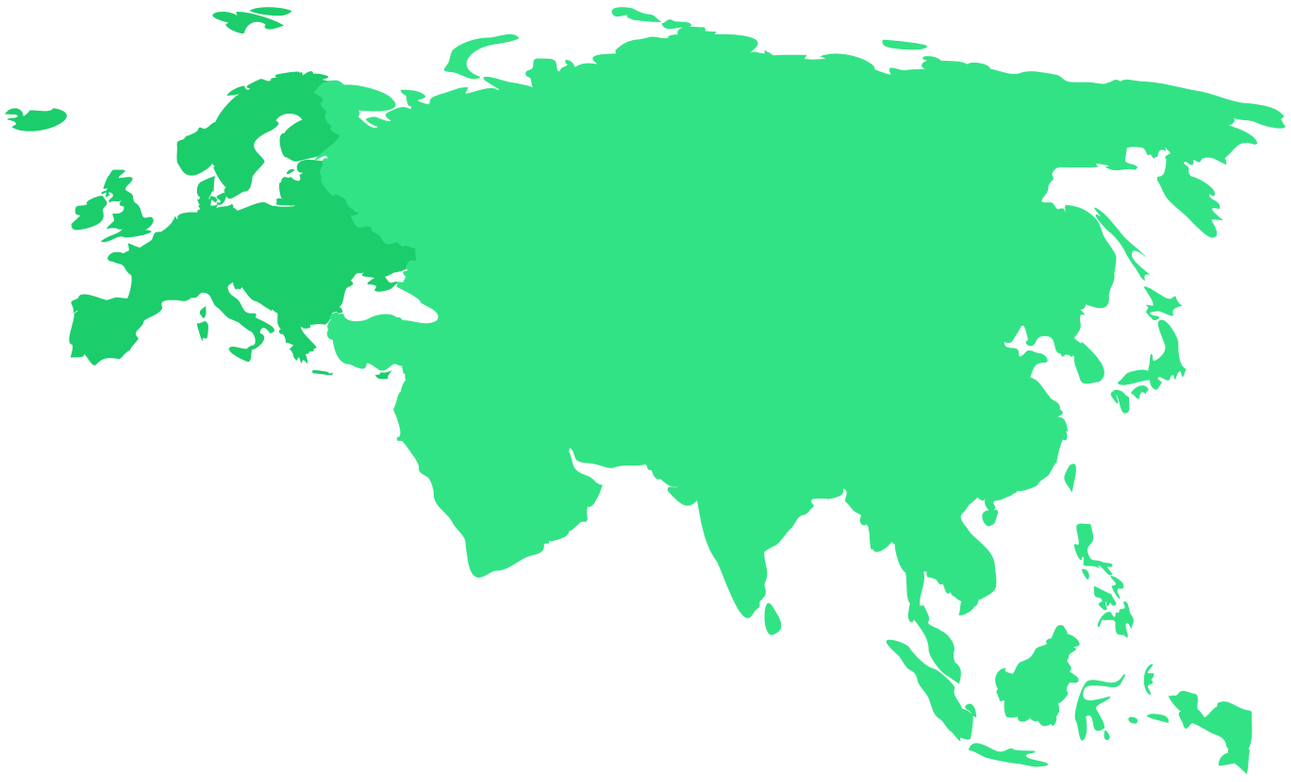
...

About BackBox

BackBox is distribution Free and Open Source, founded in 2010 by an Italian team and is designed for Ethical Hacker. Dedicated in Penetration Testing and Security Assessment.

Based on Ubuntu 04.14 LTS, it offers over 100 Tools dedicated to the world of IT Security and Computer Forensics and has a release plan scheduled every 4 months.

Look At The World



DistroWatch

BackBox is the 56th most popular Linux distribution in the world, the second most successful distribution of Penetration Testing.

37%

The 37% users of BackBox is Asian.

50k

BackBox 4.4 in 30 days got about 50,000 downloads.

Screenshot


ven 16 ott, 23:09
Information Gathering
Vulnerability Assessment
Exploitation
Privilege Escalation
Maintaining Access
Documentation & Reporting
Reverse Engineering
Social Engineering
Honeypots
Toolkit
setoolkit
Stress Testing
Automotive Analysis
Forensic Analysis
Malware Analysis
Mobile Analysis
Preferiti
Usati di recente
Tutto
Anonymous
Auditing
Services
Accessori
Grafica
Internet
Multimedia
Sistema
Sviluppo
Ufficio
Andrea
BACKBOX

Main Tools

nmap	dirs3arch	OpenVAS	ZAP
sqlmap	Metasploit	Armitage	wpscan
w3af	fang	weevely	john
Wireshark	Ettercap	wxHexEditor	setoolkit
dex2jar	aircrak-ng	can-utils	BeEF

Social and More

BackBox is present in the major social networks, on IRC and on the official website where you will find the Forum and the WiKi.

backbox.org
facebook.com/backbox.linux
twitter.com/backboxlinux
#backbox irc.autistici.org

Metasploit Framework

100%

It is a Open Source and Free project dedicated to the development and execution of exploits.

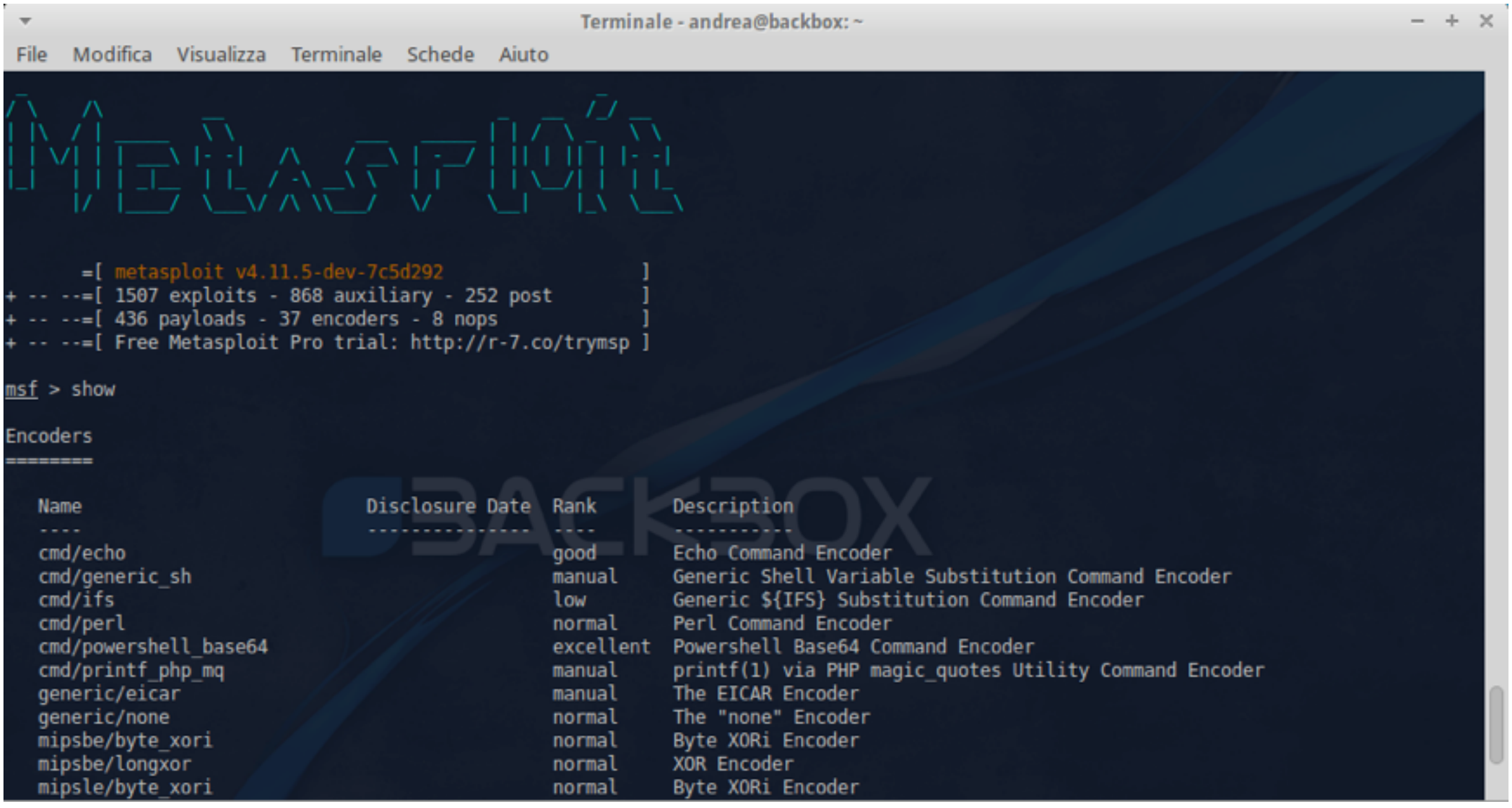
95%

It allows you to attach the 95% of operating systems vulnerable, even mobile platforms.

1500

The framework includes over 1500 Exploit for Windows, Linux, Mac, Android, iOS, etc.

Screenshot


Terminale - andrea@backbox: ~
File Modifica Visualizza Terminale Schede Aiuto
=[metasploit v4.11.5-dev-7c5d292]
+ -- --=[1507 exploits - 868 auxiliary - 252 post]
+ -- --=[436 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > show
Encoders
Name Disclosure Date Rank Description
cmd/echo good Echo Command Encoder
cmd/generic_sh manual Generic Shell Variable Substitution Command Encoder
cmd/ifs low Generic ${IFS} Substitution Command Encoder
cmd/perl normal Perl Command Encoder
cmd/powershell_base64 excellent Powershell Base64 Command Encoder
cmd/printf_php_mq manual printf(1) via PHP magic_quotes Utility Command Encoder
generic/eicar manual The EICAR Encoder
generic/none normal The "none" Encoder
mipsbe/byte_xori normal Byte XORi Encoder
mipsbe/longxor normal XOR Encoder
mipsle/byte_xori normal Byte XORi Encoder

Shellshock

CVE-2014-6271, CVE-2014-6277, CVE-2014-6278,
CVE-2014-7169, CVE-2014-7186 e CVE-2014-7187

Shellshock, also known as Bashdoor, is a vulnerability Bash Shell discovered in September 2014. Several Web services using Bash, an attacker could exploit this vulnerability to execute arbitrary commands.

Wopbot was the first botnet to use Shellshock exploit, accused of launching DDoS attacks.

1,5millions

CloudFlare has estimated that it had identified 1.5 million attacks per day.

Vectors

CGI-BIN

It is the interface between a web server and an executable that produces dynamic content; It has been identified as the main attack vector.

DHCP Clients

Some DHCP clients when authenticating welcome requests Bash.
WiFi Open can be exploited.

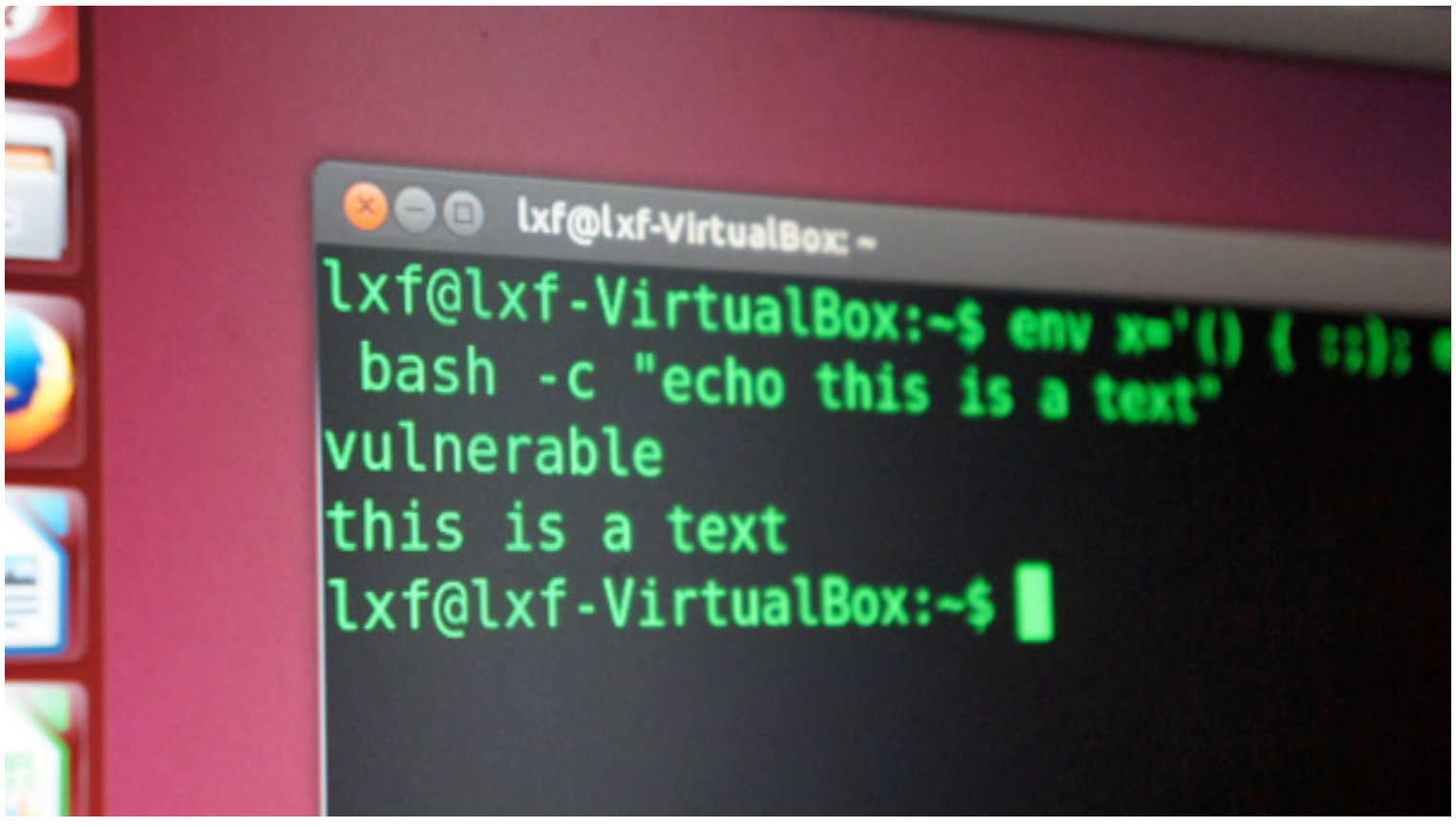
OpenSSH

OpenSSH has a function of "ForceCommand", where a default command is executed at login, allows you to execute commands without restrictions.

Qmail

When using Bash to process the mail, the mail server Qmail internally performs the commands in the external inputs.

CVE-2014-6271



env x='() { :;}; echo vulnerable' bash -c "echo this is a test"

This is the original form of vulnerability, concerns a specially created environment variable containing a function, followed by arbitrary commands.

Demonstration

Exploiting the vulnerability CVE-2014-6271 attack a vulnerable system, we will use as a carrier a CGI script in Web Server.

Test Environment:

- BackBox 4.4
- Ubuntu 12.04

Video

https://youtu.be/XDivO7DRO5w

Questions?

Credits: Opening image of CloudFlare