
**LINUXDAY 2017 Roma Tre**

# HackLab2017-3

## Linuxshell Italia

# Honeypots && Brute Force Attacks
# Offensive Security Lab

**Presenta Marco Pantò – Net Security Engineer**

http://www.linuxshell.it - http://www.certificazionilinux.com
info@linuxshell.it


**Skills**

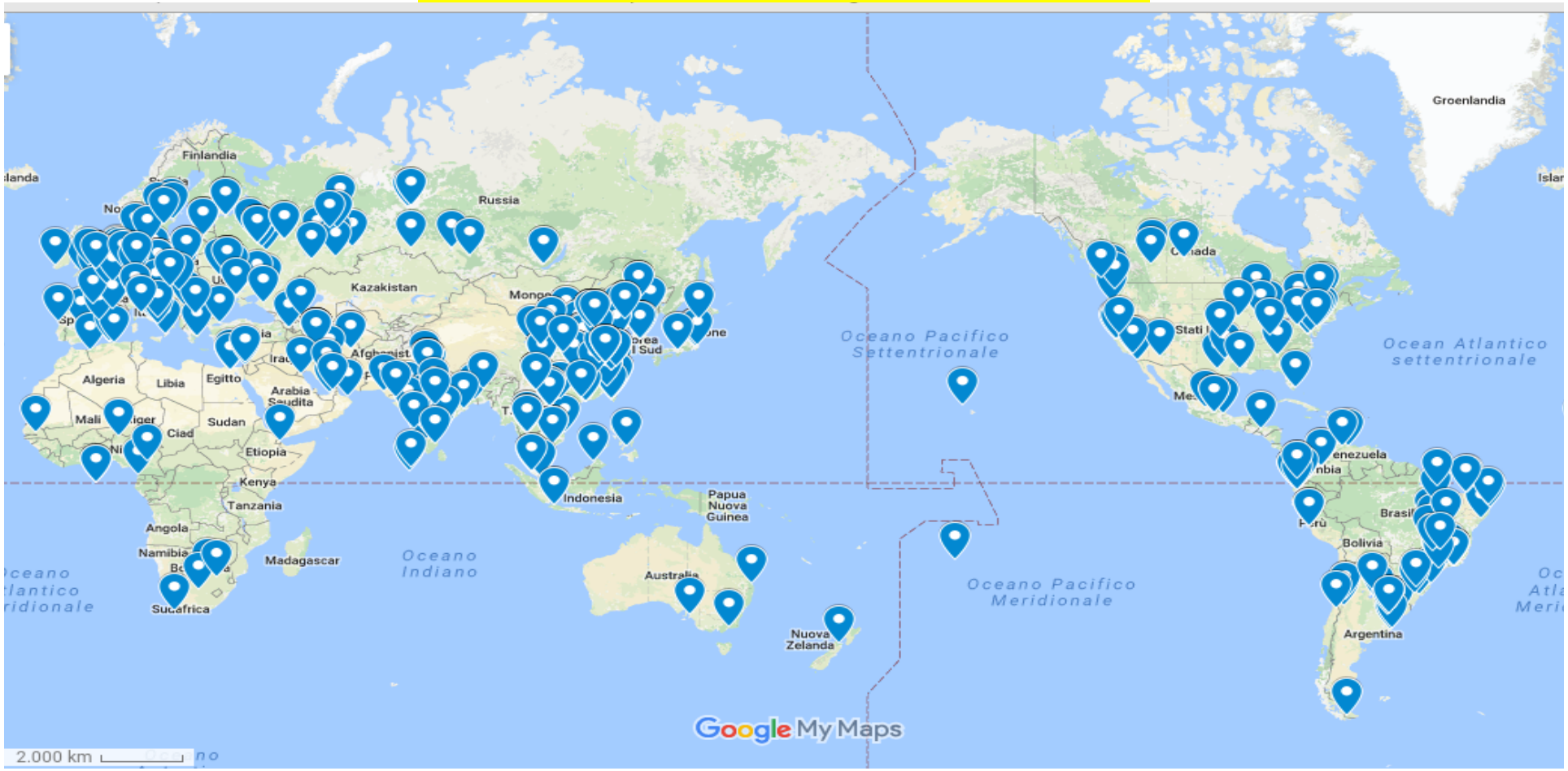
sys admin - networking - security
script bash programming
python language programmer know how base level

**Assets**

passive info gathering
enumerazione passiva
network-scan decoy
vulnerability assessment

http://www.linuxshell.it - http://www.certificazionilinux.com
info@linuxshell.it

# IDS REPORT KAMIKAZE PROJECT





http://www.linuxshell.it - http://www.certificazionilinux.com
info@linuxshell.it


# Brute Force Tools

## Hydra

**wget http://freeworld.thc.org/releases/hydra-6.3-src.tar.gz**

**PROTOCOLLI SUPPORTATI:**

**TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC, irc, RSH, RLOGIN, CVS, SNMP, SMTP, SOCKS5, VNC, POP3, IMAP, NNTP,**
**PCNFS, XMPP, ICQ, SAP/R3, LDAP2, LDAP3, Postgres, Teamspeak, Cisco auth, Cisco enable, AFP, Subversion/SVN, Firebird, LDAP2, Cisco AAA**

**hydra -l root -P passwords.txt 10.10.10.10 ssh**

http://www.linuxshell.it - http://www.certificazionilinux.com
info@linuxshell.it


## FTP

**hydra -l root -P passwords.txt 10.10.10.10 ftp**

## Medusa

**PROTOCOLLI SUPPORTATI:**

**AFP, CVS, FTP, HTTP, IMAP, MS-SQL, MySQL, NetWare NCP, NNTP, PcAnywhere, POP3, PostgreSQL, REXEC, RLOGIN, RSH, SMBNT, SMTP-AUTH, SMTP-VRFY,**
**SNMP, SSHv2, Subversion (SVN), Telnet, VMware Authentication Daemon (vmauthd), VNC,**
**Generic Wrapper,**

http://www.linuxshell.it - http://www.certificazionilinux.com
info@linuxshell.it


**Web Form**
**wget http://www.foofus.net/jmk/tools/medusa-2.0.tar.gz**

**root@wintermute:~# medusa -u root -P passwords.txt -h ip -M ssh**

**Ncrack**

**PROTOCOLLI SUPPORTATI:**

**RDP, SSH, http(s), SMB, pop3(s), VNC, FTP, telnet**

**git clone https://github.com/nmap/ncrack.git**

**root@wintermute:~# ncrack -p 22 --user root -P passwords.txt ip**


## FTP

**ncrack -u test -P passwords.txt 10.10.10.10 -p 21**

## RDP

**ncrack -u administrator -P passwords.txt -p 3389 10.212.50.21**


# PASSWORD LIST

## CRUNCH

**Crunch crea wordlist su criteri specificati**
**crunch <min> max<max> <characterset> -t <pattern> -o <output filename>**
**where min and max are numbers**

**git clone https://github.com/crunchsec/crunch.git**
**make && make install**

## OPTIONS

**-b : the maximum size of the wordlist (requires -o START)**
**-c : numbers of lines to write to the wordlist (requires -o START)**
**-d : limit the number of duplicate characters**
**-e : stop generating words at a certain string**

**-f : specify a list of character sets from the charset.lst file**
**-i : invert the order of characters in the wordlist**
**-l : allows the literal interpretation of @,%^ when using -t**
**-o : the output wordlist file**
**-p : print permutations without repeating characters (cannot be used with -s)**
**-q : Like the -p option except it reads the strings from a specified file**
**-r : resume a previous session (cannot be used with -s)**
**-s : specify a particular string to begin the wordlist with**
**-t : set a specific pattern of @,%^**
**-z : compress the output wordlist file, accompanied by -o**