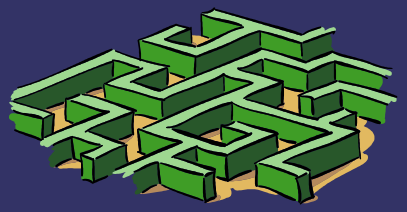
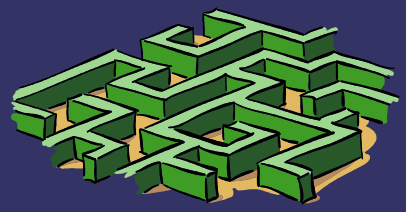
Tehnike napada na WEB servise #2

“Oružje u pogrešnim rukama”



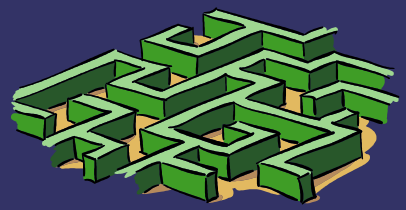
Tema

- Koncentrisanje na grupu koja izaziva najviše štete na mreži;
- Neznanje kao produkt upijanja znanja;
- Korišćenje gotovih alata za ugrožavanje online sigurnosti;
- Na kraju uvek ostave trag.



Script Kiddies

- Termin skiddie I podela po nivou “znanja”;
- Zašto su opasni?
- Razmišljaj destruktivno, ne etički.
- “Znam šta radim, ali pojma nemam kako.”
- Posledice... Nisu moja stvar.

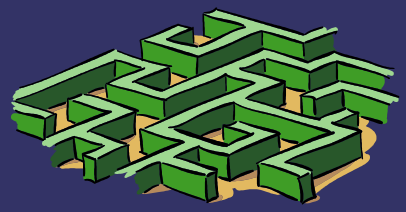


*Linux/*BSD ol d vej*

- Protecting your server against script kiddie attacks

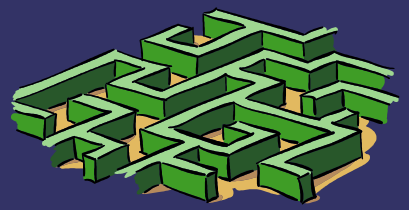
Oruzije skiddija

- “Hack” forumi izobilje malware-a, I software-a pravljenog za ometanje sigurnosti.
- Tutorijali za korišćenje, bez pomena funkcionisanja.
- Masovne međusobne infekcije I backdoor-ovi.
- Alati za pentesting/ testiranje sigurnosti, skiddie koriste van lokalne testing mreže.
- Popularne pentesting distribucije: BackTrack I sada Kali Linux.
- Exploiti(javni uglavnom)



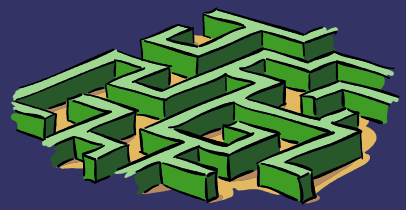
Mete skiddija

- Ko najviše strada? Obični korisnici;
- Najčešće mete korisnici Windows OS-a;
- Malware infekcije, problem koji se izuzetnom brzinom širi mrežom.
- Servisi skladištenja fajlova, I grupacije sajtova gde se masovno preuzimaju fajlovi;



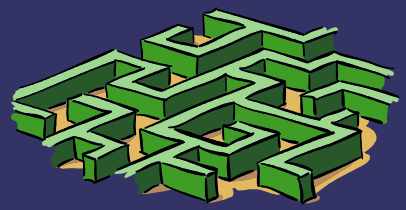
Exploits

- “Program” koji koristi rupu na sistemu;
- Većina pisana u C-u;
- Remote I Local exploiti, različito mesto izvršavanja;
- Dok god bude software-a, biće exploita.
- Najveći deo exploita bazira se na stack overflow-u;
- Privatni(0day) I javni exploiti.



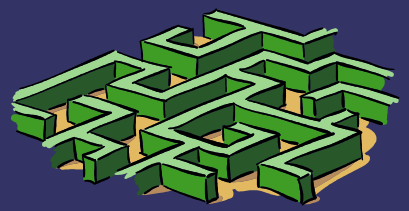
Buffer overflow

- Ovaj deo skiddie ne zna;
- Prepunjavanje stack-a prebacuje EIP na memorijsku lokaciju gde stavljamo naš shell kod;
- Buffer overflowAko u niz[4] unesemo 6 elemenata, šta se dešava?
- Cilj izvršavanja shell koda u neautorizovanom memori-jskom prostoru; Sa super permisijama;



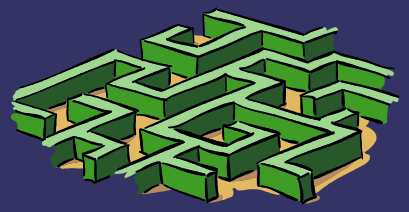
Javni exploiti

- Verovatno je patch oslobođen;
- Exploit-DB I 1337day, najveći mirrori;
- Dostupne čitave arhive za download;
- Metasploit framework za pentestere (~1060 exploita);



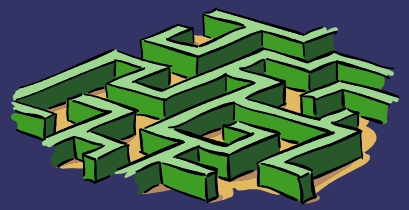
U napad

- Muzika Iz filma hackers u pozadini
- Brze naočare
- Kapuljača na glavi, godišnje doba nije bitno;
- Red bull ili neko drugo brzo energetsko piće;
- Majica sa natpisom: 1m 5k1dd13 bu7 31337



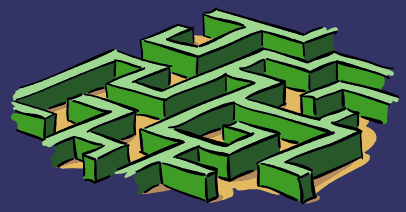
Nacin razmisljanja SK-a

- Prva metoda old skul bruteforce;
- Hydra remote crack alat I krekovanje SSH;
- Druga metoda ranjivost web sajta (SQLi za primer);
- SQLMAP I ranjivost ne filtrirane interakcije PHP-a I MySQL-a



Hydra cracker I SSH

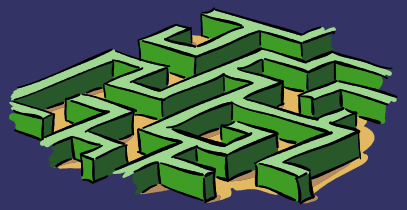
- THC-Hydra program za krekovanje logon sistema;
- Podržava dosta protokola;
- Koristi wordliste;
- Generisanje wordlisti sa alatom crunch;
- Ima podršku za ubacivanje modula.



Podrzani protokoli

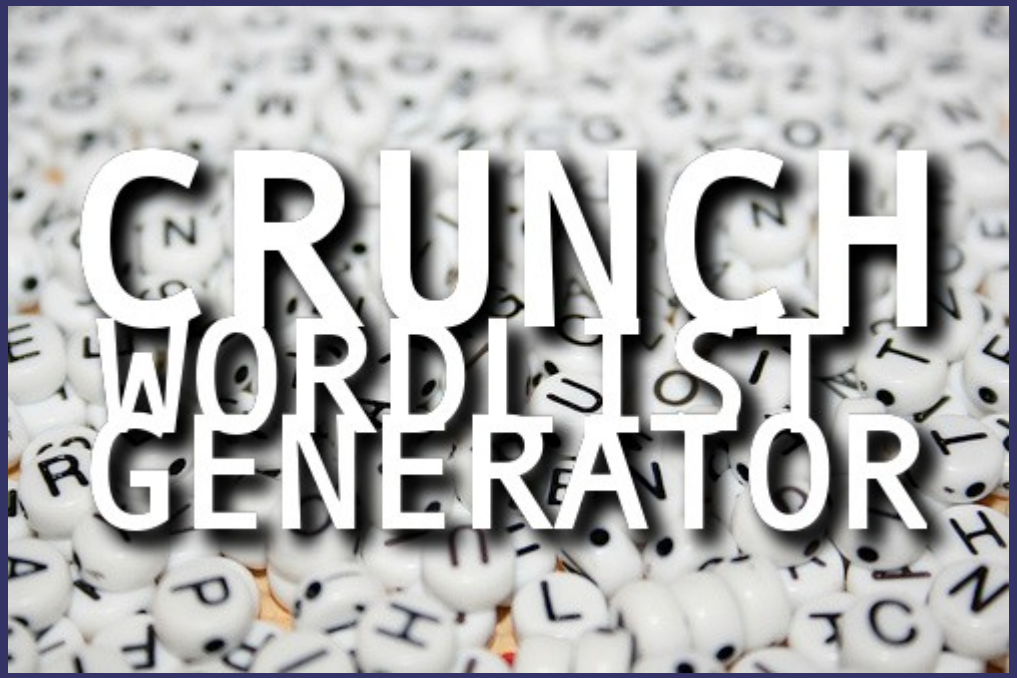
Lista:

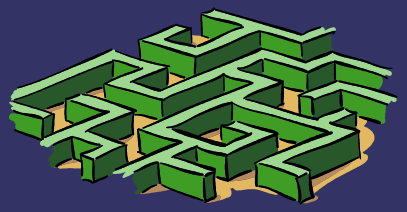
- Afp
- Cisco
- Cisco-enable
- Cvs
- Firebird
- Ftp
- Ftps
- http[s]-{head|get}
- http[s]-{get|post}-form
- Http-proxy
- Http-proxy-urlenum
- Icq
- imap[s]
- Irc
- ldap2[s
- ldap3[-{cram|digest}md5][s]
- Mssql
- Mysq
- Ssh
- Sshkey
- Vnc
- xmpp
- Ncp
- Nntp
- Oracle-listener
- Oracle-sid
- Pcanywhere
- Pcnfs
- pop3[s]
- Postgres
- Rdp
- Rexec
- Rlogin
- Rsh
- Sip
- Smb
- smtp[s]
- Smtp-enum
- Snmp
- Socks5
- Svn
- Teamspeak
- telnet[s]
- vmauthd



Crunch generator

- Crunch generator wordlista;
- Generiše sa parametrima za minimalni broj karaktera, maksimalni broj, I charset.





Napad 1 - bruteforce

Alati:

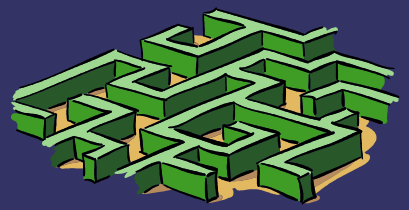
- THC-Hydra
- Nmap scanner
- Crunch wordlist creator
- Weevely backdoor

Meta:

- Server: Ubuntu
- Kernel: 2.6.32
- Server je VM
- IP:provericemo :)
- Meta za krekovanje: SSH server.

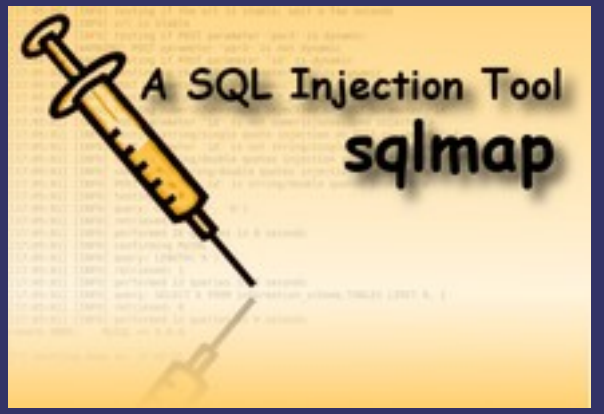
Opis

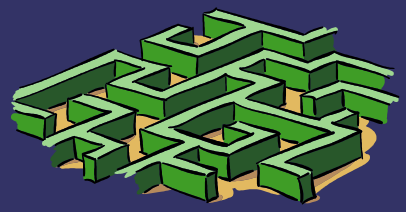
- Jedan od administratora servera ima očajnu lozinku, korisničko ime mu je **test** I rizikuje da bude žrtva brutfors napada.



SQLMAP alat

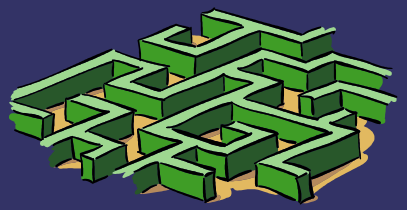
- Alat koji istražuje propuste u formama koje napadaču omogućuju interakciju sa sistemom za upravljanje baza podataka;
- Mogućnost povezivanja na proxy;
- Remote dump baze podaka;
- Više platformska podrška.
- --wizard

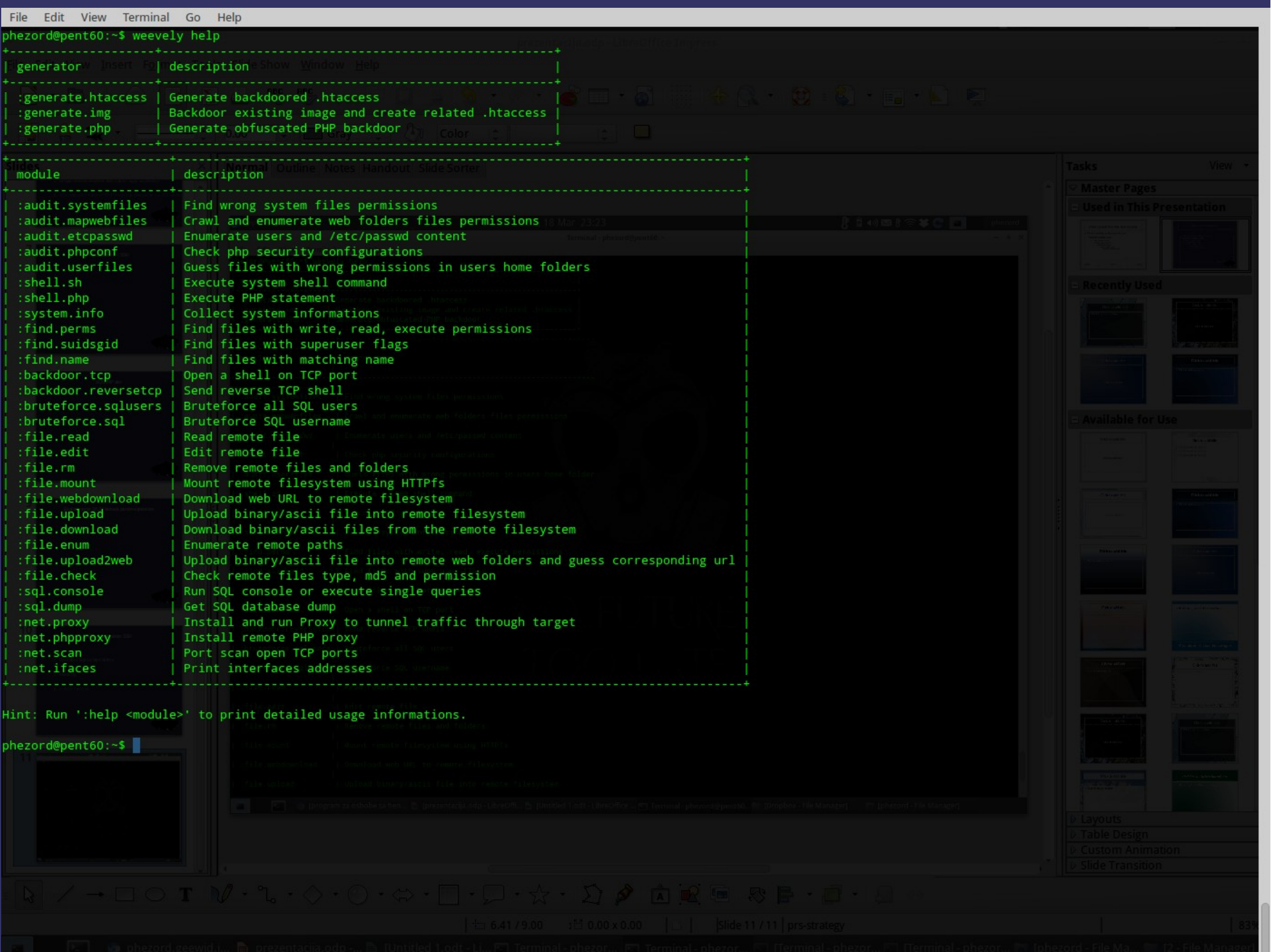




Weevely simulator SSH

- Backdoor koji se lepo skriva;
- Mana tty;
- Puno funkcija;
- Više opcija pri izboru generisanja playload-a.




File Edit View Terminal Go Help
phezord@pent60:~$ weevely help
generator	description
:generate.htaccess	Generate backdoored .htaccess
:generate.img	Backdoor existing image and create related .htaccess
:generate.php	Generate obfuscated PHP backdoor
module	description
:audit.systemfiles	Find wrong system files permissions
:audit.mapwebfiles	Crawl and enumerate web folders files permissions
:audit.etcpasswd	Enumerate users and /etc/passwd content
:audit.phpconf	Check php security configurations
:audit.userfiles	Guess files with wrong permissions in users home folders
:shell.sh	Execute system shell command
:shell.php	Execute PHP statement
:system.info	Collect system informations
:find.perms	Find files with write, read, execute permissions
:find.suidsgid	Find files with superuser flags
:find.name	Find files with matching name
:backdoor.tcp	Open a shell on TCP port
:backdoor.reversetcp	Send reverse TCP shell
:bruteforce.sqlusers	Bruteforce all SQL users
:bruteforce.sql	Bruteforce SQL username
:file.read	Read remote file
:file.edit	Edit remote file
:file.rm	Remove remote files and folders
:file.mount	Mount remote filesystem using HTTPfs
:file.webdownload	Download web URL to remote filesystem
:file.upload	Upload binary/ascii file into remote filesystem
:file.download	Download binary/ascii files from the remote filesystem
:file.enum	Enumerate remote paths
:file.upload2web	Upload binary/ascii file into remote web folders and guess corresponding url
:file.check	Check remote files type, md5 and permission
:sql.console	Run SQL console or execute single queries
:sql.dump	Get SQL database dump
:net.proxy	Install and run Proxy to tunnel traffic through target
:net.phpproxy	Install remote PHP proxy
:net.scan	Port scan open TCP ports
:net.ifaces	Print interfaces addresses
Hint: Run ':help <module>' to print detailed usage informations.
phezord@pent60:~$

Prakticni napad 2 – error based SQLi kroz SQLMAP

Alati:

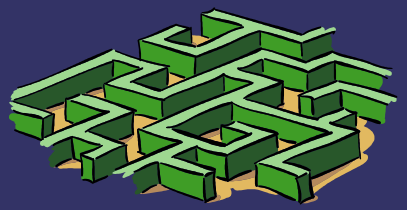
- SQLMAP
- Weevely backdoor
- Local Privilege Escalation Exploit [<=2.6.37]

Meta:

- Server: Ubuntu
- Kernel: 2.6.32
- Server je VM
- IP:provericemo :)
- Meta za krekovanje: SSH server.

Opis

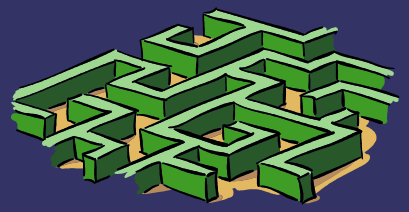
- SQLMAP automatizuje proces eksploatacije;
- Upload backdoor.
- Treći alat: local root exploit;



Exploitovanje kernela javnim exploitom
Dobijanje root privilegija

- Javni exploit sa exploit-db;
- Poprilično star;

- Kernel <= 2.6.37;
- Postoji patch za isti kernel koji sprečava izvršavanje;



LUGoNS Barcamp #2

$ cat end.txt

- Autor: Strahinja Piperac