enum4linux Cheat Sheet ∞

CHEAT-SHEET 29 Mar 2015  Arr0way

enum4linux is an alternative to enum.exe on Windows, enum4linux is used to enumerate Windows and Samba hosts.

enum4linux in a nutshell

- RID cycling (When RestrictAnonymous is set to 1 on Windows 2000)
- User listing (When RestrictAnonymous is set to 0 on Windows 2000)
- Listing of group membership information

All Blog
Cheat Sheets
Techniques
Security Hardening
WalkThroughs

CHEAT SHEETS

Penetration Testing Tools Cheat Sheet
LFI Cheat Sheet
Vi Cheat Sheet
Systemd Cheat Sheet
Reverse Shell Cheat Sheet
nbtscan Cheat Sheet
Nmap Cheat Sheet
Linux Commands Cheat Sheet

- Share enumeration
- Detecting if host is in a workgroup or a domain
- Identifying the remote operating system
- Password policy retrieval (using polenum)

enum4linux Cheat Sheet

COMMAND	DESCRIPTION
`enum4linux -v target-ip`	Verbose mode, shows the underlying commands being executed by enum4linux
`enum4linux -a target-ip`	Do Everything, runs all options apart from dictionary based share name guessing
`enum4linux -U target-ip`	Lists usernames, if the server allows it - (RestrictAnonymous = 0)
`enum4linux -u administrator -p password -U target-ip`	If you've managed to obtain credentials, you can pull a full list of users regardless of the RestrictAnonymous option
`enum4linux -r target-ip`	Pulls usernames from the default RID range (500-550,1000-1050)

More »

WALKTHROUGHS

InsomniHack CTF Teaser - Smartcat2 Writeup
InsomniHack CTF Teaser - Smartcat1 Writeup
FristiLeaks 1.3 Walkthrough
SickOS 1.1 - Walkthrough
The Wall Boot2Root Walkthrough
More »

TECHNIQUES

SSH & Meterpreter Pivoting Techniques
More »

SECURITY HARDENING

Security Harden CentOS 7
More »

`enum4linux -R 600-660 target-ip`	Pull usernames using a custom RID range
`enum4linux -G target-ip`	Lists groups. if the server allows it, you can also specify username `-u` and password `-p`
`enum4linux -S target-ip`	List Windows shares, again you can also specify username `-u` and password `-p`
`enum4linux -s shares.txt target-ip`	Perform a dictionary attack, if the server doesn't let you retrieve a share list
`enum4linux -o target-ip`	Pulls OS information using smbclient, this can pull the service pack version on some versions of Windows
`enum4linux -i target-ip`	Pull information about printers known to the remove device.

/DEV/URANDOM

MacBook - Post Install Config + Apps

More »

OTHER BLOG

HowTo: Kali Linux Chromium Install for Web App Pen Testing

Jenkins RCE via Unauthenticated API

MacBook - Post Install Config + Apps

enum4linux Cheat Sheet

Linux Local Enumeration Script

HowTo Install Quassel on Ubuntu

HowTo Install KeepNote on OSX Mavericks

Follow Arr0way

Twitter GitHub

Also...

You might want to read these

CATEGORY	POST NAME
cheat-sheet	Penetration Testing Tools Cheat Sheet
cheat-sheet	LFI Cheat Sheet
kali linux	HowTo: Kali Linux Chromium Install for Web App Pen Testing
walkthroughs	InsomniHack CTF Teaser - Smartcat2 Writeup

walkthroughs	InsomniHack CTF Teaser - Smartcat1 Writeup
walkthroughs	FristiLeaks 1.3 Walkthrough
walkthroughs	SickOS 1.1 - Walkthrough
walkthroughs	The Wall Boot2Root Walkthrough
walkthroughs	/dev/random: Sleepy Walkthrough CTF
walkthroughs	/dev/random Pipe walkthrough