



INCIDENT RESPONSE CHEATSHEET WINDOWS & LINUX

Table of Contents

Abstract	5
Linux Incident Response	6
What is Incident Response?	7
User Accounts	7
/etc/passwd	7
passwd -S	8
grep	8
find /-nouser	8
/etc/shadow	9
/etc/group	10
/etc/sudoers	11
Log Entries	12
Lastlog	12
Auth.log	12
History	13
System Resources	14
Uptime	14
Free	14
/proc/memory	14
/proc/mounts	15
Processes	15
top	15
ps aux	16
PID	16
Services	17
Service	17
/etc/cronjob	18
/etc/resolv.conf	18
/etc/hosts	19
iptables	19
Files	20

Large Files	20
mtime	20
Network Settings	21
ifconfig	21
Open files	21
netstat	22
arp	22
path	22
Windows Incident Response	23
Users	24
Local users	24
Net user	25
net localgroup	25
Local user	26
Processes	26
Task Manager	26
tasklist	27
Powershell	28
Services	30
GUI	30
net Start	30
sc query	31
Task Scheduler	32
tasklist	32
GUI	32
Schtasks	33
Startup	33
GUI	33
Powershell	34
Registry	35
GUI	35
PowerShell	36
Active TCP and UDP Port	36
netstat	36

Powershell	37
File Sharing	38
net view	38
SMBShare	38
Files	39
Forfiles	39
Firewall Settings	41
Sessions with other system	42
Open Sessions	43
Log Enteries	43
Event Viewer	43
Cmd	44
PowerShell	44
Conclusion	45
References	45
About Us	46

Abstract

For some people who use their computer systems, their systems might seem normal to them, but they might never realise that there could be something really fishy or even that fact that their systems could have been compromised. Making use of Incident Response a large number of attacks at the primary level could be detected. The investigation can be carried out to obtain any digital evidence.

Detecting any intrusion in your system is a very important step towards Incident response. Incident response is quite vast, but it is always better to start small. While performing incident response, you should always focus on suspected systems and the areas where it seems there could be a breach. Making use of Incident Response, you could detect a large number of attacks at the primary level.

The purpose of incident response is nothing but Live Forensics. The investigation can be carried out to obtain any digital evidence. This article mainly focuses on how incident response can be performed in a Linux system. So, to get you started with this cheat sheet, switch on your Linux machine and open the terminal to accomplish these commands.