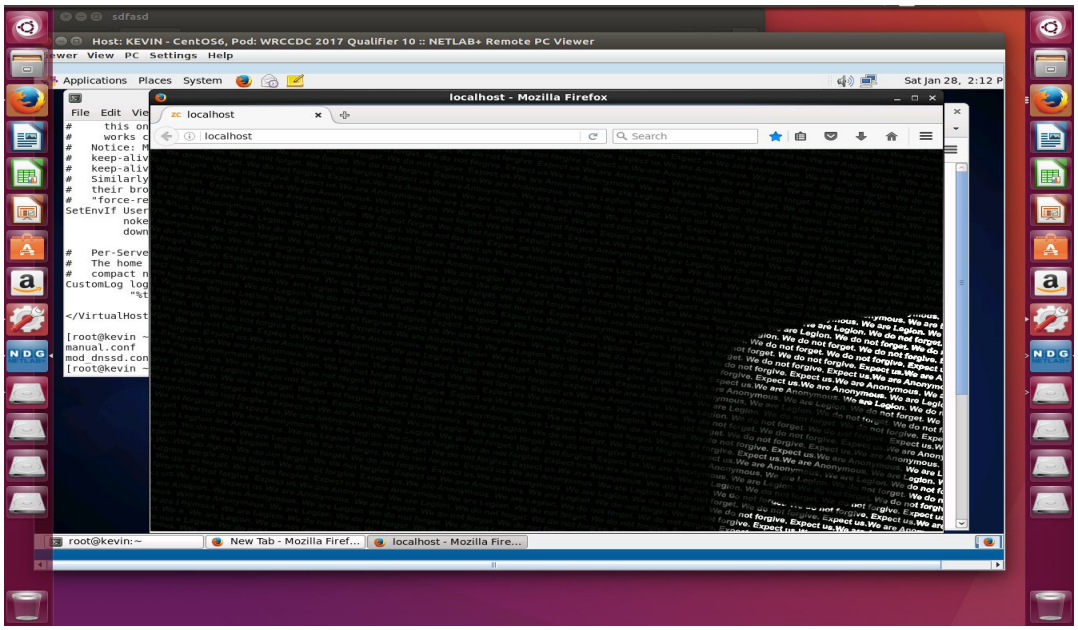
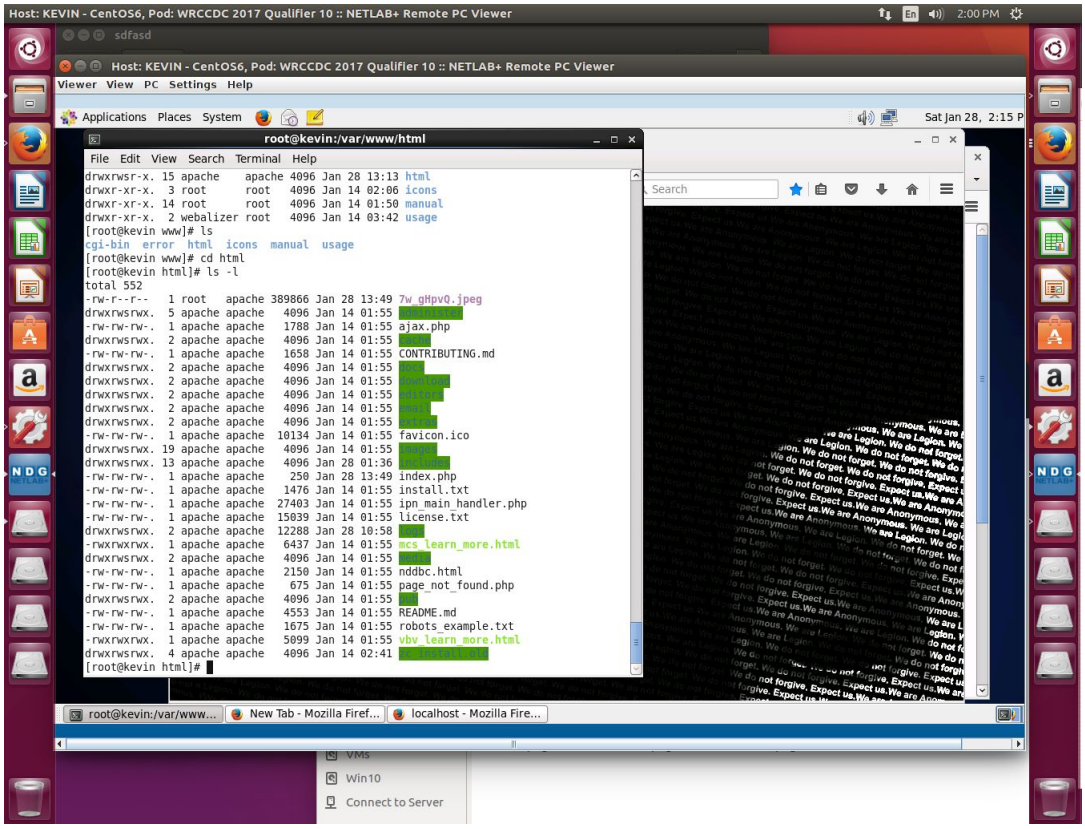
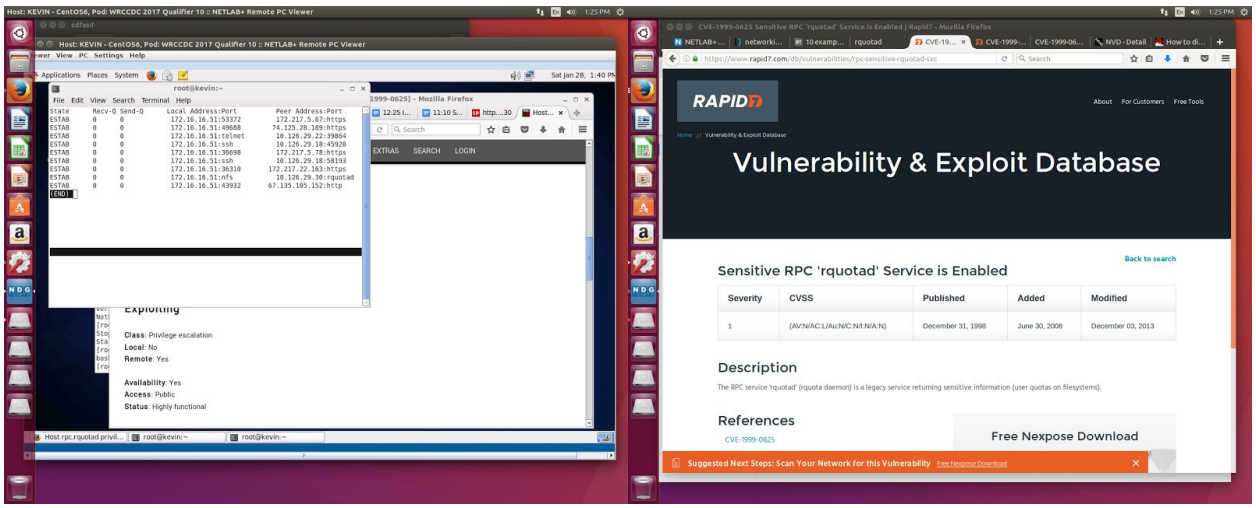
CentOS - ECommerce site compromised





This screen capture shows the image on ecommerce site changed at 1:49 pm

Host rpc.rquotad privilege escalation



https://vuldb.com/?id.14392

https://www.rapid7.com/db/vulnerabilities/rpc-sensitive-rquotad-svc

CVE-1999-0625

A vulnerability classified as critical was found in Host (the affected version is unknown). This vulnerability affects an unknown function of the component *rpc.rquotad*. The manipulation with an unknown input leads to a privilege escalation vulnerability. As an impact it is known to affect confidentiality, integrity, and availability.
The weakness was disclosed 01/01/1999. This vulnerability was named CVE-1999-0625. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details are unknown but a public exploit is available.
It is declared as highly functional. The vulnerability scanner Nessus provides a plugin with the ID 10226 (rquotad Service Detection), which helps to determine the existence of the flaw in a target environment. It is assigned to the family *RPC*. The commercial vulnerability scanner Qualys is able to test this issue with plugin 66047.
It is possible to mitigate the problem by applying the configuration setting .

- Suspicious connection on CentOS, need to dig further:

ESTAB 0 0 172.16.16.51:nfs 10.126.29.30:rquotad

Rquotad is an rpc(3N) server which returns quotas for a user of a local filesystem, which is mounted by a remote machine over the NFS. It also allows setting of quotas on NFS mounted Filesystems

As shown here, a private IP of 10.26.29.xx is connected via ssh + telnet, and running rquotad

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
ESTAB	0	0	172.16.16.51:53372	172.217.5.67:https
ESTAB	0	0	172.16.16.51:49688	74.125.28.189:https
ESTAB	0	0	172.16.16.51:telnet	10.126.29.22:39864
ESTAB	0	0	172.16.16.51:ssh	10.126.29.18:45928
ESTAB	0	0	172.16.16.51:36698	172.217.5.78:https
ESTAB	0	0	172.16.16.51:ssh	10.126.29.18:58193
ESTAB	0	0	172.16.16.51:36310	172.217.22.163:https
ESTAB	0	0	172.16.16.51:nfs	10.126.29.30:rquotad
ESTAB	0	0	172.16.16.51:43932	67.135.105.152:http

(END)