



Houston

Ethan, Lazaro, Zanovia, Chris

Oct 4, 2023

18:36 First signs of activity

```
Oct  4 18:36:24 cnt-dmz-apache2 sshd[10603]: Connection closed by invalid user admin 199.203.100.23
port 38231 [preauth]
Oct  4 18:36:24 cnt-dmz-apache2 sshd[10704]: Invalid user user from 199.203.100.233 port 44745
Oct  4 18:36:24 cnt-dmz-apache2 sshd[10704]: pam_unix(sshd:auth): authentication failure; logname= u
id=0 euid=0 tty=ssh ruser= rhost=199.203.100.233
Oct  4 18:36:26 cnt-dmz-apache2 sshd[10704]: Failed password for invalid user user from 199.203.100.
233 port 44745 ssh2
Oct  4 18:36:27 cnt-dmz-apache2 sshd[10704]: Connection closed by invalid user user 199.203.100.233
port 44745 [preauth]
Oct  4 18:36:27 cnt-dmz-apache2 sshd[10717]: pam_unix(sshd:auth): authentication failure; logname= u
id=0 euid=0 tty=ssh ruser= rhost=199.203.100.233 user=root
Oct  4 18:36:29 cnt-dmz-apache2 sshd[10717]: Failed password for root from 199.203.100.233 port 3549
5 ssh2
Oct  4 18:36:30 cnt-dmz-apache2 sshd[10717]: Connection closed by authenticating user root 199.203.1
00.233 port 35495 [preauth]
Oct  4 18:36:30 cnt-dmz-apache2 sshd[10735]: Accepted password for root from 199.203.100.233 port 36
763 ssh2
Oct  4 18:38:14 cnt-dmz-apache2 sshd[11582]: Accepted password for root from 199.203.100.233 port 43
373 ssh2
Oct  4 18:39:38 cnt-dmz-apache2 sshd[11582]: Received disconnect from 199.203.100.233 port 43373:11:
Connection terminated by the client.
Oct  4 18:39:38 cnt-dmz-apache2 sshd[11582]: Disconnected from user root 199.203.100.233 port 43373
root@cnt-dmz-apache2:/var/log#
```



18:43 First signs of activity caught in QRadar

Oct 4, 2023, 6:43:42 PM	 199.203.100.233	32805	 130.2.1.22	22	tcp_ip	RemoteAccess.SSH
Oct 4, 2023, 6:43:42 PM	 199.203.100.233	44649	 130.2.1.22	22	tcp_ip	RemoteAccess.SSH
Oct 4, 2023, 6:43:42 PM	 199.203.100.233	35537	 130.2.1.22	22	tcp_ip	RemoteAccess.SSH
Oct 4, 2023, 6:43:42 PM	 199.203.100.233	46291	 130.2.1.22	22	tcp_ip	RemoteAccess.SSH
Oct 4, 2023, 6:43:42 PM	 199.203.100.233	32815	 130.2.1.22	22	tcp_ip	RemoteAccess.SSH
Oct 4, 2023, 6:43:41 PM	192.168.110.110	53400	192.168.200.1	53	udp_ip	Misc.domain

18:53 QRadar Alert: Port Scan Detected

All Offenses > Offense 41 (Summary)

Offense 41

Magnitude	<div><div></div><div></div><div></div><div></div></div>	Status		Relevance	1
Description	Port Scan Detected containing Traffic End	Offense Type		Destination IP	
		Event/Flow count		644 events and 0 flows in 2 categories	
Source IP(s)	 199.203.100.233	Start		Oct 4, 2023, 6:53:48 PM	
Destination IP(s)	 130.2.1.22	Duration		42s	
Network(s)	other	Assigned to		Unassigned	



Offense Source Summary

IP  130.2.1.22

18:57 Password guessing

All Offenses > Offense 42 (Summary)

Offense 42

Magnitude	
Description	Password Guessing containing User failed to login to SSH
Source IP(s)	 199.203.100.233
Destination IP(s)	172.16.100.22 (cnt-dmz-apache2.services.dom)
Network(s)	DMZ.Internal

Offense Source Summary

IP	172.16.100.22
----	---------------

19:03 Apache2 service domain has been hacked



Threat actor not in our system

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 127.0.0.1:53            0.0.0.0:*
tcp        0      0 0.0.0.0:22              0.0.0.0:*
tcp6       0      0 :::80                   :::*
tcp6       0      0 :::22                   :::*
```

Threat actor never got passed the CNT Firewall

The screenshot displays the PA-VM web interface. The top navigation bar includes the PA-VM logo and tabs for DASHBOARD, ACC, MONITOR (active), POLICIES, OBJECTS, NETWORK, and DEVICE. A 'Commit' button is visible on the right. Below the navigation bar, a search bar contains the filter '{ addr.src in 199.203.100.233 }'. The left sidebar shows a tree view with 'Logs' expanded, listing various log categories such as Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Tunnel Inspection, Configuration, System, Alarms, Authentication, and Unified. The main content area shows a table with columns: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, SOURCE USER, SOURCE DYNAMIC ADDRESS GROUP, DESTINATION, and DE. The table is currently empty.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DE.
--------------	------	-----------	---------	--------	-------------	------------------------------	-------------	-----

19:05 hacked2z.png in apache2 domain (ogani.com)

```
</html>root@cnt-dmz-apache2:/var/www/ogani# ls
blog-details.html  contact.html  hacked2z.png  js          sass          shopping-cart.html
blog.html          css          img          main.html  shop-details.html  Source
checkout.html     fonts        index.html   readme.txt  shop-grid.html
root@cnt-dmz-apache2:/var/www/ogani# cat hacked2z.png
cat: hacked2z.png: No such file or directory
root@cnt-dmz-apache2:/var/www/ogani#
```



19:50 Threat Actor Left Firewall

forgot screenshot sorry :)