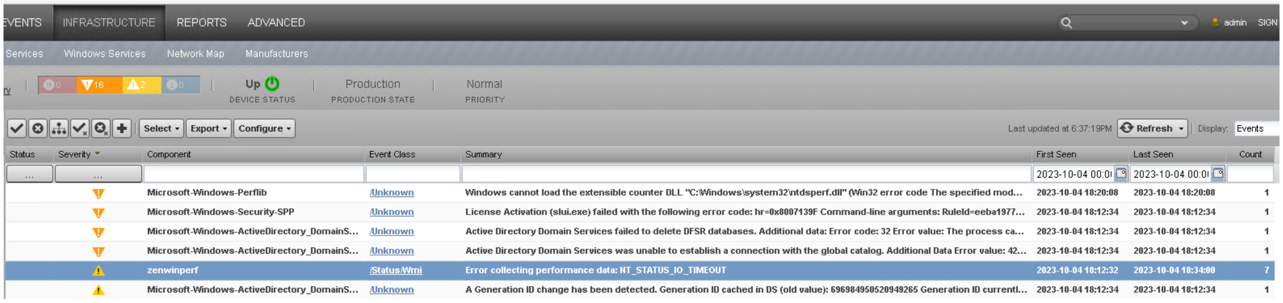
Windsor Day 2: Web Defacement

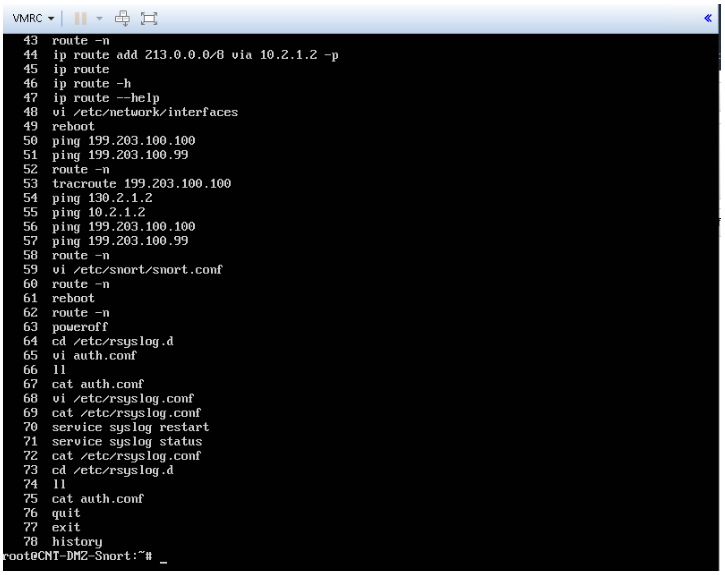
Disclaimer: Cyber Range does not allow file transfers so all information is stored as screenshots

18:12 - 18:29 4 errors, 2 Warnings in Zenoss

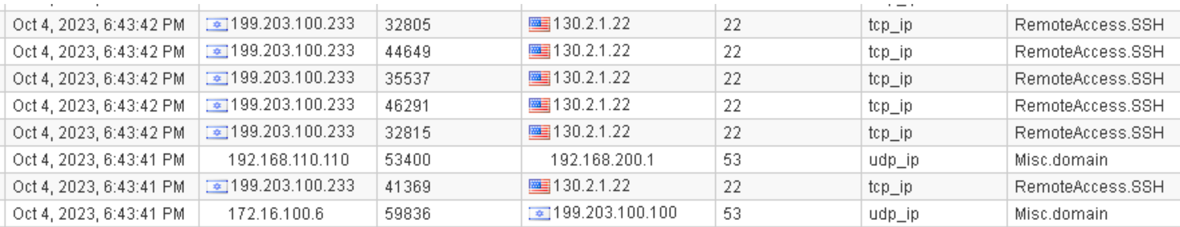


Status	Severity	Component	Event Class	Summary	First Seen	Last Seen	Count
...	...				2023-10-04 00:0	2023-10-04 00:0	
	▼	Microsoft-Windows-Perflib	/Unknown	Windows cannot load the extensible counter DLL "C:\Windows\system32\ntdsperf.dll" (Win32 error code The specified mod...	2023-10-04 18:20:08	2023-10-04 18:20:08	1
	▼	Microsoft-Windows-Security-SPP	/Unknown	License Activation (slui.exe) failed with the following error code: hr=0x8007139F Command-line arguments: RuleId=eeba1977...	2023-10-04 18:12:34	2023-10-04 18:12:34	1
	▼	Microsoft-Windows-ActiveDirectory_DomainS...	/Unknown	Active Directory Domain Services failed to delete DFSR databases. Additional data: Error code: 32 Error value: The process ca...	2023-10-04 18:12:34	2023-10-04 18:12:34	1
	▼	Microsoft-Windows-ActiveDirectory_DomainS...	/Unknown	Active Directory Domain Services was unable to establish a connection with the global catalog. Additional Data Error value: 42...	2023-10-04 18:12:34	2023-10-04 18:12:34	1
	⚠	zenwinperf	/Status/Wmi	Error collecting performance data: NT_STATUS_IO_TIMEOUT	2023-10-04 18:12:32	2023-10-04 18:34:00	7
	⚠	Microsoft-Windows-ActiveDirectory_DomainS...	/Unknown	A Generation ID change has been detected. Generation ID cached in DS (old value): 696984950520949265 Generation ID currentl...	2023-10-04 18:12:34	2023-10-04 18:12:34	1

18:43 199.203.100.x First contact with Snort (IPS/IDS)

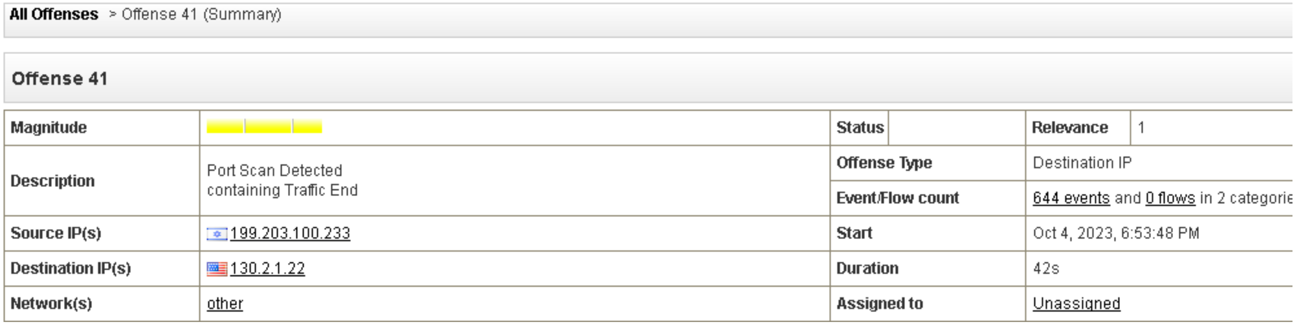


```
  43  route -n
  44  ip route add 213.0.0.0/8 via 10.2.1.2 -p
  45  ip route
  46  ip route -h
  47  ip route --help
  48  vi /etc/network/interfaces
  49  reboot
  50  ping 199.203.100.100
  51  ping 199.203.100.99
  52  route -n
  53  tracroute 199.203.100.100
  54  ping 130.2.1.2
  55  ping 10.2.1.2
  56  ping 199.203.100.100
  57  ping 199.203.100.99
  58  route -n
  59  vi /etc/snort/snort.conf
  60  route -n
  61  reboot
  62  route -n
  63  poweroff
  64  cd /etc/rsyslog.d
  65  vi auth.conf
  66  ll
  67  cat auth.conf
  68  vi /etc/rsyslog.conf
  69  cat /etc/rsyslog.conf
  70  service syslog restart
  71  service syslog status
  72  cat /etc/rsyslog.conf
  73  cd /etc/rsyslog.d
  74  ll
  75  cat auth.conf
  76  quit
  77  exit
  78  history
root@CNT-DMZ-Snort:~# _
```



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
Oct 4, 2023, 6:43:41 PM	199.203.100.233	41369	130.2.1.22	22	tcp_ip	RemoteAccess.SSH
Oct 4, 2023, 6:43:41 PM	172.16.100.6	59836	199.203.100.100	53	udp_ip	Misc.domain

18:53 Port scan detected

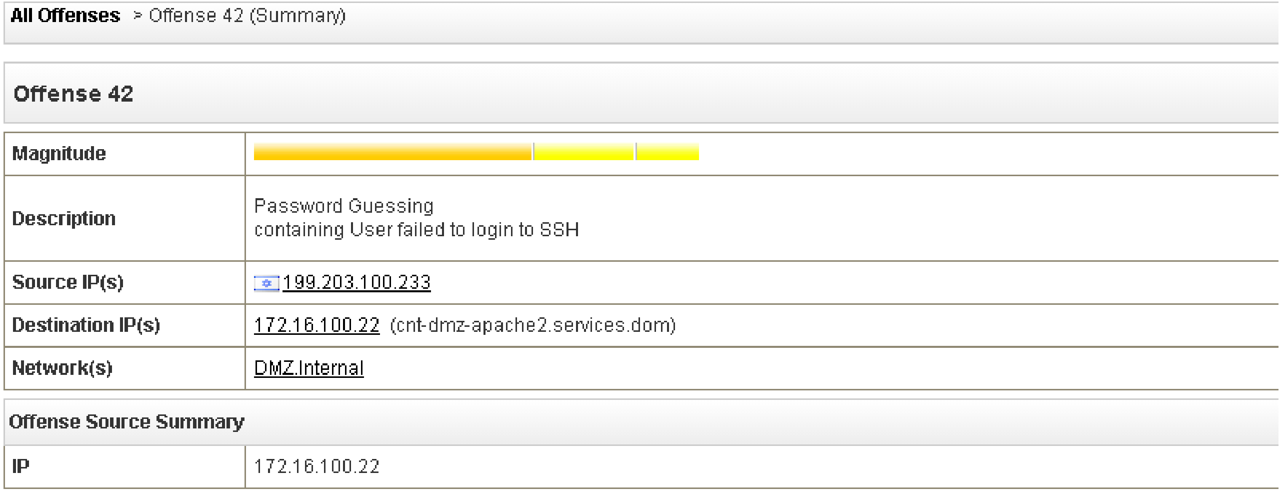


All Offenses > Offense 41 (Summary)

Offense 41

Magnitude		**Status**		**Relevance**	1
Description	Port Scan Detected containing Traffic End	**Offense Type**	Destination IP		
		Event/Flow count	644 events and 0 flows in 2 categorie		
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		

18:57 password guessing containing user failed to login to SSH



All Offenses > Offense 42 (Summary)

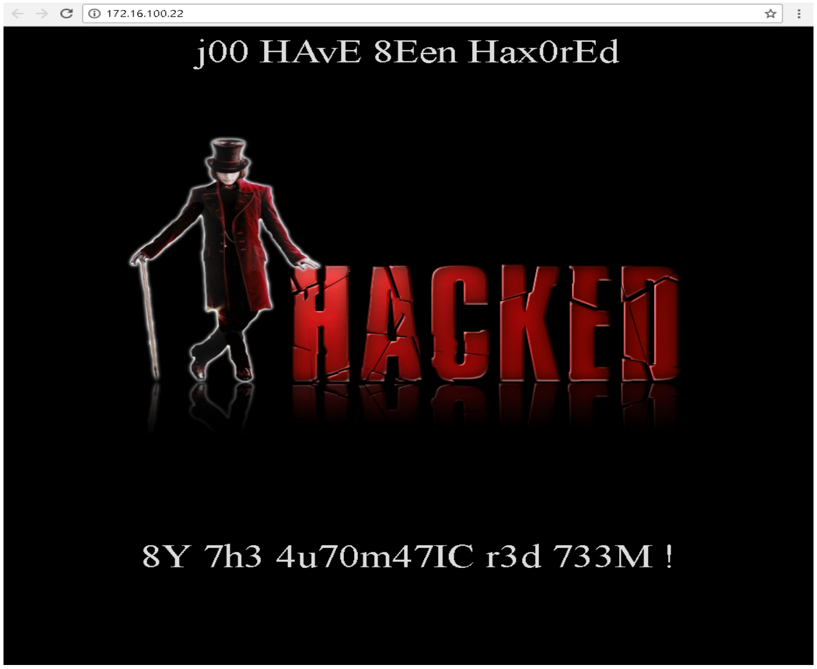
Offense 42

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

Apache2 website (ogani.com) has been defaced (172.16.100.22)

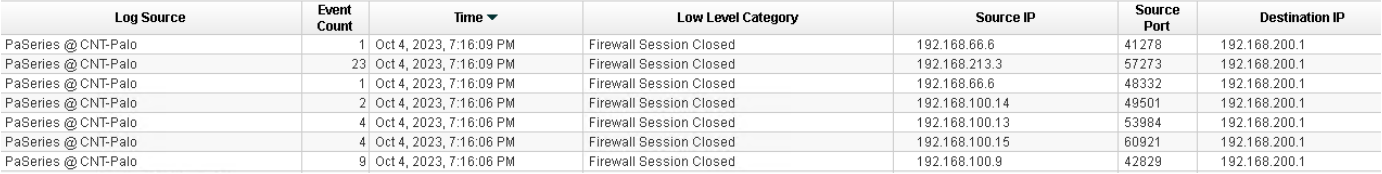


172.16.100.22

j00 HAvE 8Een Hax0rEd

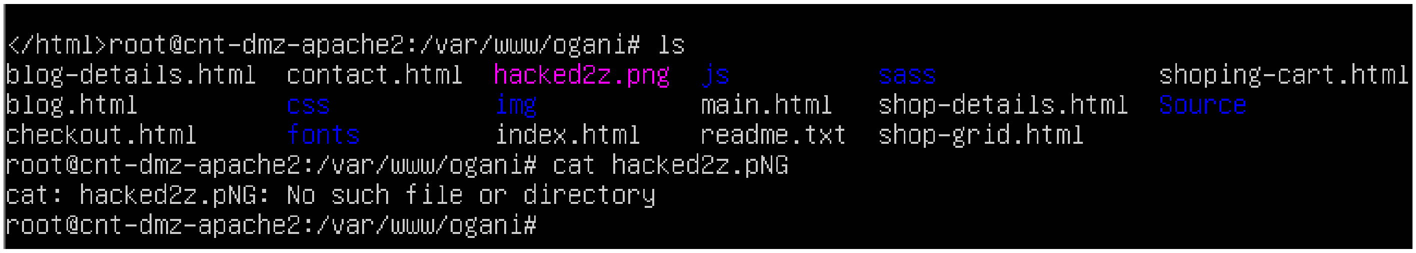
8Y 7h3 4u70m47IC r3d 733M !

19:16 Firewall Session Closed (192.168.100.9,14,13,15)



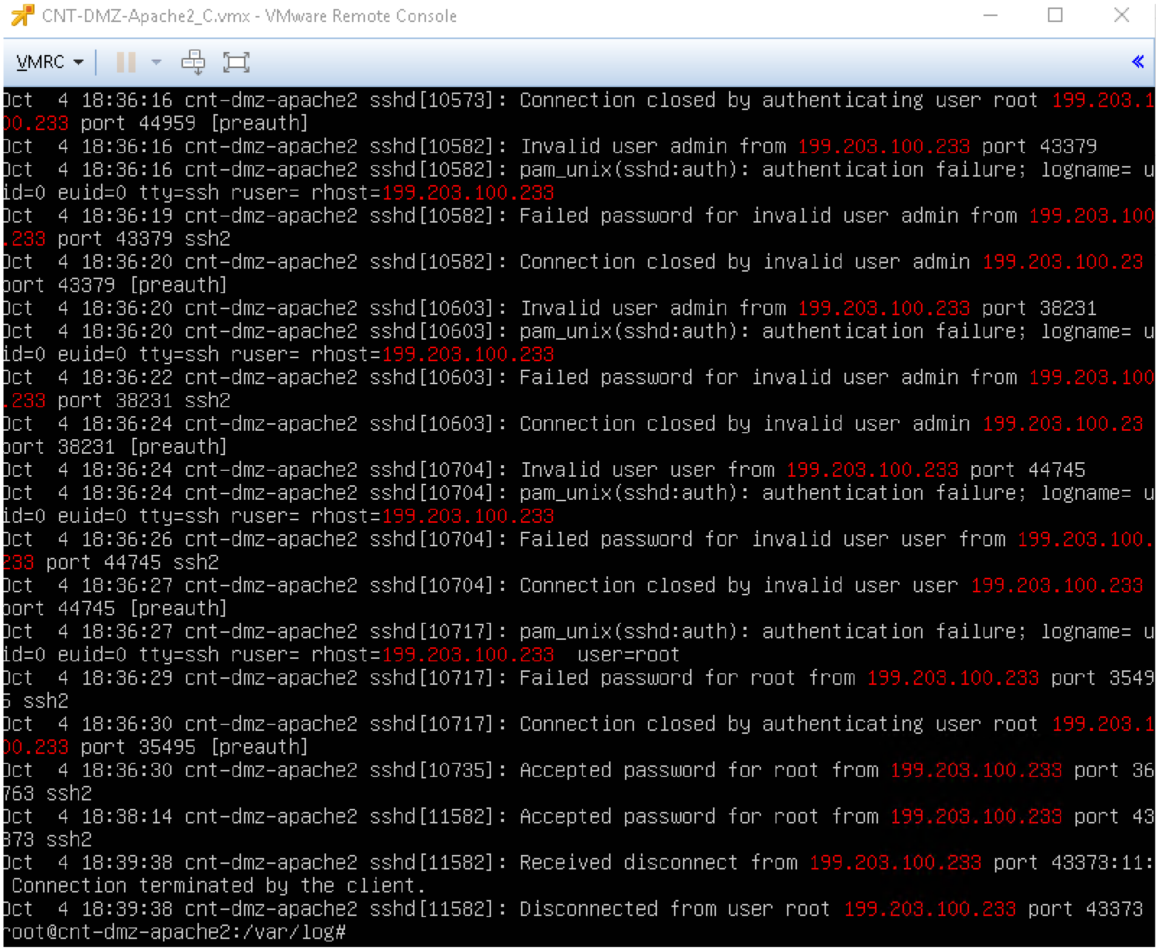
Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP
PaSeries @ CNT-Palo	1	Oct 4, 2023, 7:16:09 PM	Firewall Session Closed	192.168.66.6	41278	192.168.200.1
PaSeries @ CNT-Palo	23	Oct 4, 2023, 7:16:09 PM	Firewall Session Closed	192.168.213.3	57273	192.168.200.1
PaSeries @ CNT-Palo	1	Oct 4, 2023, 7:16:09 PM	Firewall Session Closed	192.168.66.6	48332	192.168.200.1
PaSeries @ CNT-Palo	2	Oct 4, 2023, 7:16:06 PM	Firewall Session Closed	192.168.100.14	49501	192.168.200.1
PaSeries @ CNT-Palo	4	Oct 4, 2023, 7:16:06 PM	Firewall Session Closed	192.168.100.13	53984	192.168.200.1
PaSeries @ CNT-Palo	4	Oct 4, 2023, 7:16:06 PM	Firewall Session Closed	192.168.100.15	60921	192.168.200.1
PaSeries @ CNT-Palo	9	Oct 4, 2023, 7:16:06 PM	Firewall Session Closed	192.168.100.9	42829	192.168.200.1

Uploaded 2Z.png into HTML code in Apache2 website (ogani.com)



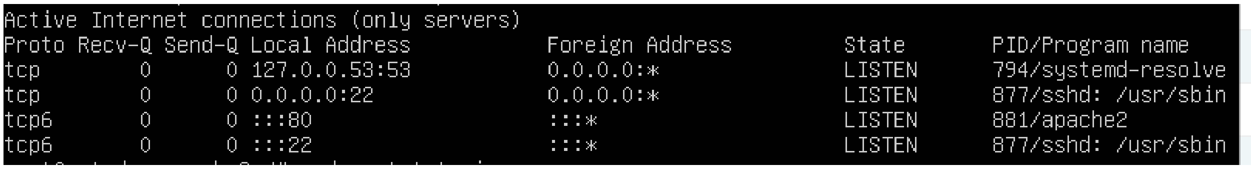
```
</html>root@cnt-dmz-apache2:/var/www/ogani# ls
blog-details.html  contact.html  hacked2z.png  js         sass               shoping-cart.html
blog.html          css           img           main.html  shop-details.html  Source
checkout.html      fonts         index.html    readme.txt shop-grid.html
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#
```

199.203.100.233 Brute forces into Apache2 Server (password was P@ssw0rd)



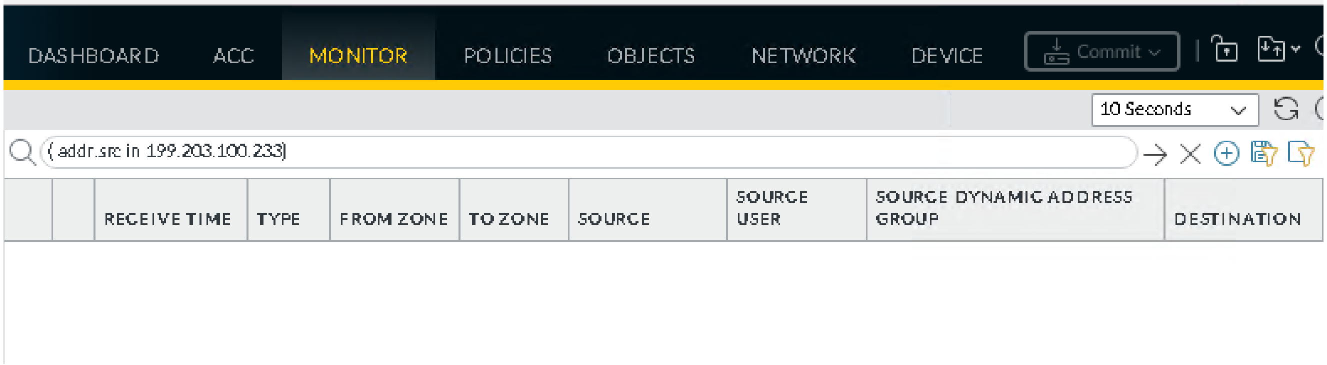
```
Oct  4 18:36:16 cnt-dmz-apache2 sshd[10573]: Connection closed by authenticating user root 199.203.1
00.233 port 44959 [preauth]
Oct  4 18:36:16 cnt-dmz-apache2 sshd[10582]: Invalid user admin from 199.203.100.233 port 43379
Oct  4 18:36:16 cnt-dmz-apache2 sshd[10582]: pam_unix(sshd:auth): authentication failure; logname= u
id=0 euid=0 tty=ssh ruser= rhost=199.203.100.233
Oct  4 18:36:19 cnt-dmz-apache2 sshd[10582]: Failed password for invalid user admin from 199.203.100
.233 port 43379 ssh2
Oct  4 18:36:20 cnt-dmz-apache2 sshd[10582]: Connection closed by invalid user admin 199.203.100.23
port 43379 [preauth]
Oct  4 18:36:20 cnt-dmz-apache2 sshd[10603]: Invalid user admin from 199.203.100.233 port 38231
Oct  4 18:36:20 cnt-dmz-apache2 sshd[10603]: pam_unix(sshd:auth): authentication failure; logname= u
id=0 euid=0 tty=ssh ruser= rhost=199.203.100.233
Oct  4 18:36:22 cnt-dmz-apache2 sshd[10603]: Failed password for invalid user admin from 199.203.100
.233 port 38231 ssh2
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#
```

Threat actor not in system



```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      794/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      877/sshd: /usr/sbin
tcp6       0      0 :::80                   :::*                    LISTEN      881/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      877/sshd: /usr/sbin
```

Threat as far as we know localized to the DMZ (no traffic through CNT firewall)



(addr.src in 199.203.100.233)

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