

Lab 1: HTB Starting Point Machines

Machine 2: Fawn

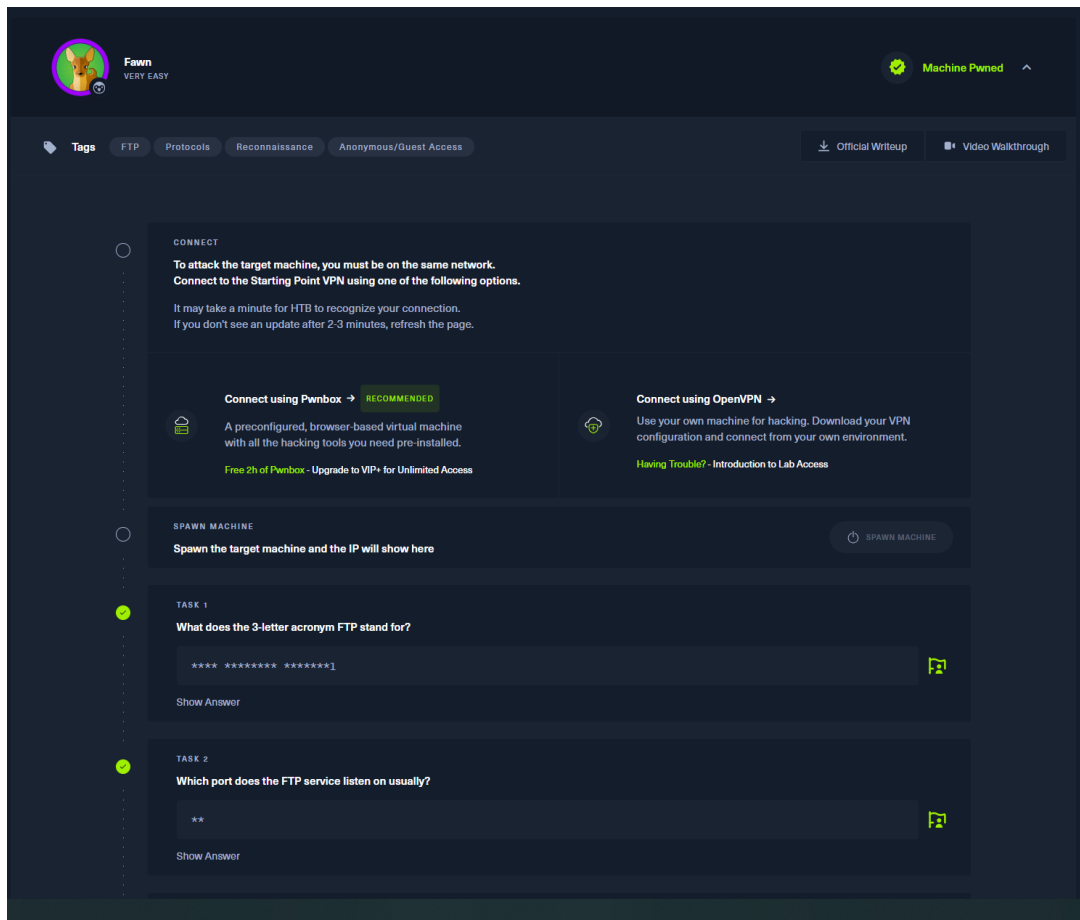
Technical Details:

- Open Ports: 21 (FTP)
- Service: vsftpd 3.0.3
- Vulnerability: Anonymous FTP login enabled

Network connectivity was verified using the **ping** command. An **Nmap** scan was conducted to identify open ports, revealing that the FTP service was running on **port 21**.

Anonymous login access was found to be enabled on the FTP service, allowing unauthorized entry. The **ls** command was used to enumerate the contents of the directory, leading to the discovery of the **flag.txt** file. The **get** command was executed to retrieve the flag, successfully completing the task.

Screenshot of the machine:



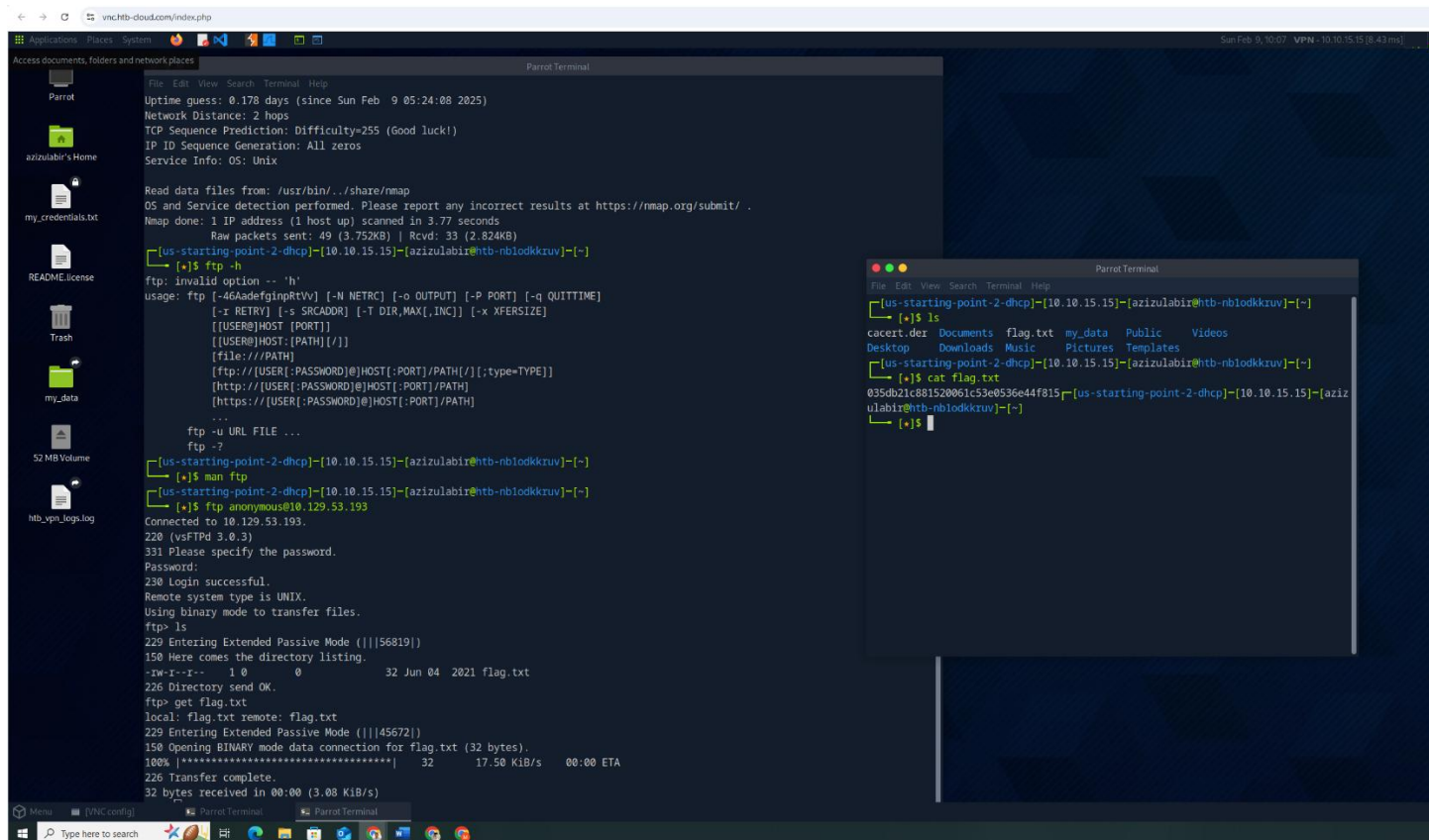
Screenshot showing the retrieved flag:

```
Parrot Terminal
File Edit View Search Terminal Help
[us-starting-point-2-dhcp]--[10.10.15.15]--[azizulabir@htb-nblodkkrub]--[~]
[*]$ nmap 10.129.53.193
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-09 09:22 CST
Nmap scan report for 10.129.53.193
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
[us-starting-point-2-dhcp]--[10.10.15.15]--[azizulabir@htb-nblodkkrub]--[~]
[*]$ nmap -sV -sS -O -v -p 21 10.129.53.193
nmap: unrecognized option '-O'
See the output of nmap -h for a summary of options.
[us-starting-point-2-dhcp]--[10.10.15.15]--[azizulabir@htb-nblodkkrub]--[~]
[*]$ ^C
[us-starting-point-2-dhcp]--[10.10.15.15]--[azizulabir@htb-nblodkkrub]--[~]
[*]$ nmap -sV -sS -O -v -p 21 10.129.53.193
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-09 09:40 CST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 09:40
Scanning 10.129.53.193 [4 ports]
Completed Ping Scan at 09:40, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:40
Completed Parallel DNS resolution of 1 host. at 09:40, 0.00s elapsed
Initiating SYN Stealth Scan at 09:40
Scanning 10.129.53.193 [1 port]
Discovered open port 21/tcp on 10.129.53.193
Completed SYN Stealth Scan at 09:40, 0.03s elapsed (1 total ports)
Initiating Service scan at 09:40
Scanning 1 service on 10.129.53.193
Completed Service scan at 09:40, 0.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.129.53.193
Retrying OS detection (try #2) against 10.129.53.193
NSE: Script scanning 10.129.53.193.
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Nmap scan report for 10.129.53.193
Host is up (0.0087s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), L
inux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.
```



Machine 3: Dancing

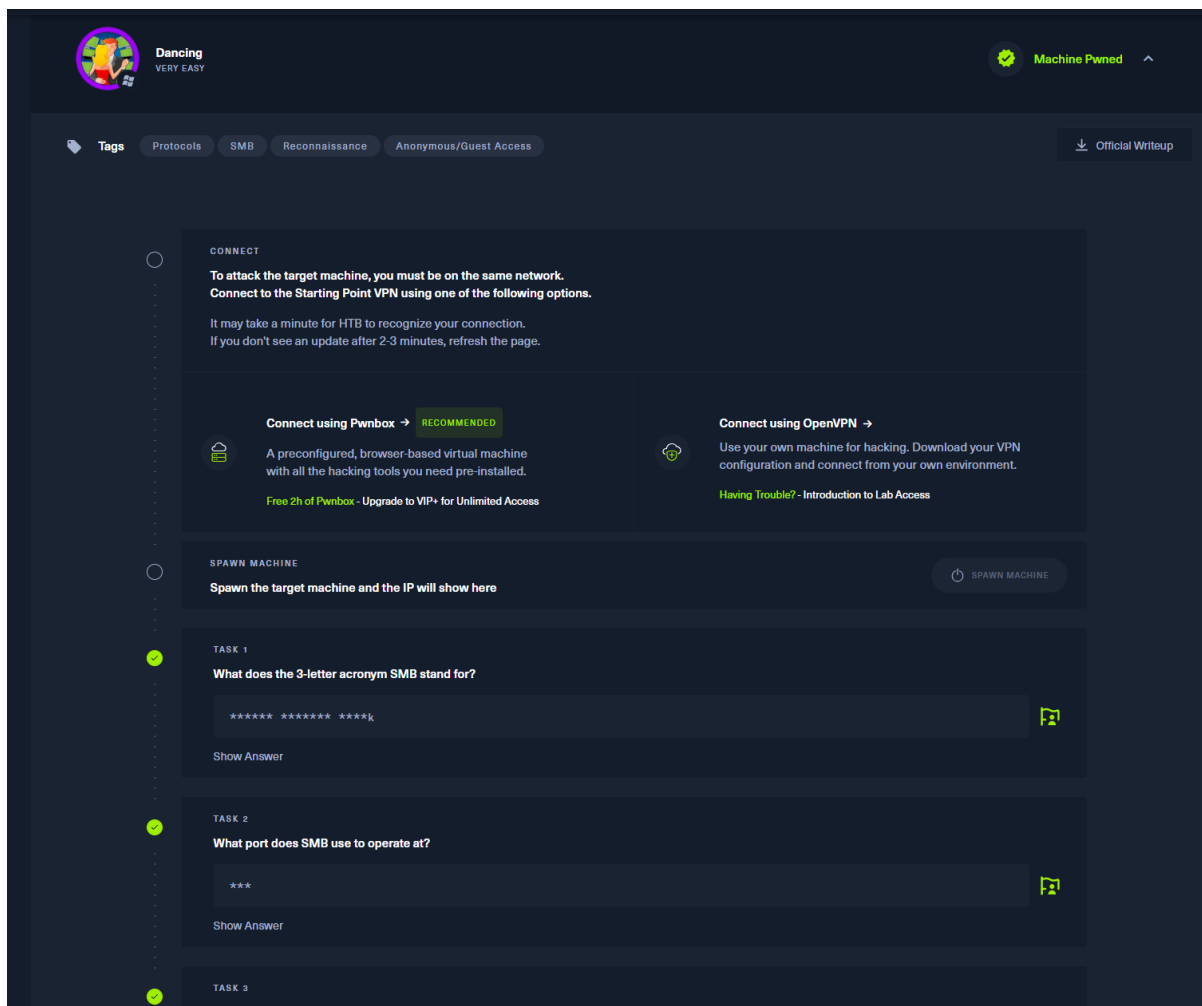
Technical Details:

- Open Ports: 445 (SMB)
- Service: Microsoft SMB (NetBIOS & Microsoft-ds)
- Vulnerability: Anonymous SMB access enabled

A connectivity check was performed using the **ping** command, confirming that the victim machine was reachable. An **nmap** scan revealed that the SMB service was running on **port 445**, identified as **Microsoft SMB (NetBIOS & Microsoft-ds)**.

Anonymous access was found to be enabled on the SMB service. Exploiting this misconfiguration, the **smbclient** tool was used to list available shares. The **ls** command was then used to enumerate shared files, leading to the discovery of the **flag.txt** file. The **get** command was executed to retrieve the flag, marking the completion of the task.

Screenshot of the machine:



Screenshot showing the retrieved flag:

```
Parrot Terminal
File Edit View Search Terminal Help

..                               D      0 Mon Mar 29 04:08:24 2021
worknotes.txt                   A      94 Fri Mar 26 06:00:37 2021

5114111 blocks of size 4096. 1752992 blocks available
smb: \Amy.J\> get worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \Amy.J\> cd ..
smb: \> ls
.                               D      0 Mon Mar 29 03:22:01 2021
..                              D      0 Mon Mar 29 03:22:01 2021
Amy.J                           D      0 Mon Mar 29 04:08:24 2021
James.P                         D      0 Thu Jun  3 03:38:03 2021

5114111 blocks of size 4096. 1752990 blocks available
smb: \> cd James.P
smb: \James.P\> ls
.                               D      0 Thu Jun  3 03:38:03 2021
..                              D      0 Thu Jun  3 03:38:03 2021
flag.txt                        A      32 Mon Mar 29 04:26:57 2021

5114111 blocks of size 4096. 1752990 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.6 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \James.P\> exit
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nblodkkrurv]-[~]
[*]$ ls
cacert.der Documents flag.txt my_data Public Videos
Desktop Downloads Music Pictures Templates worknotes.txt
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nblodkkrurv]-[~]
[*]$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nblodkkrurv]-[~]
[*]$
```

Machine 4: Redeemer

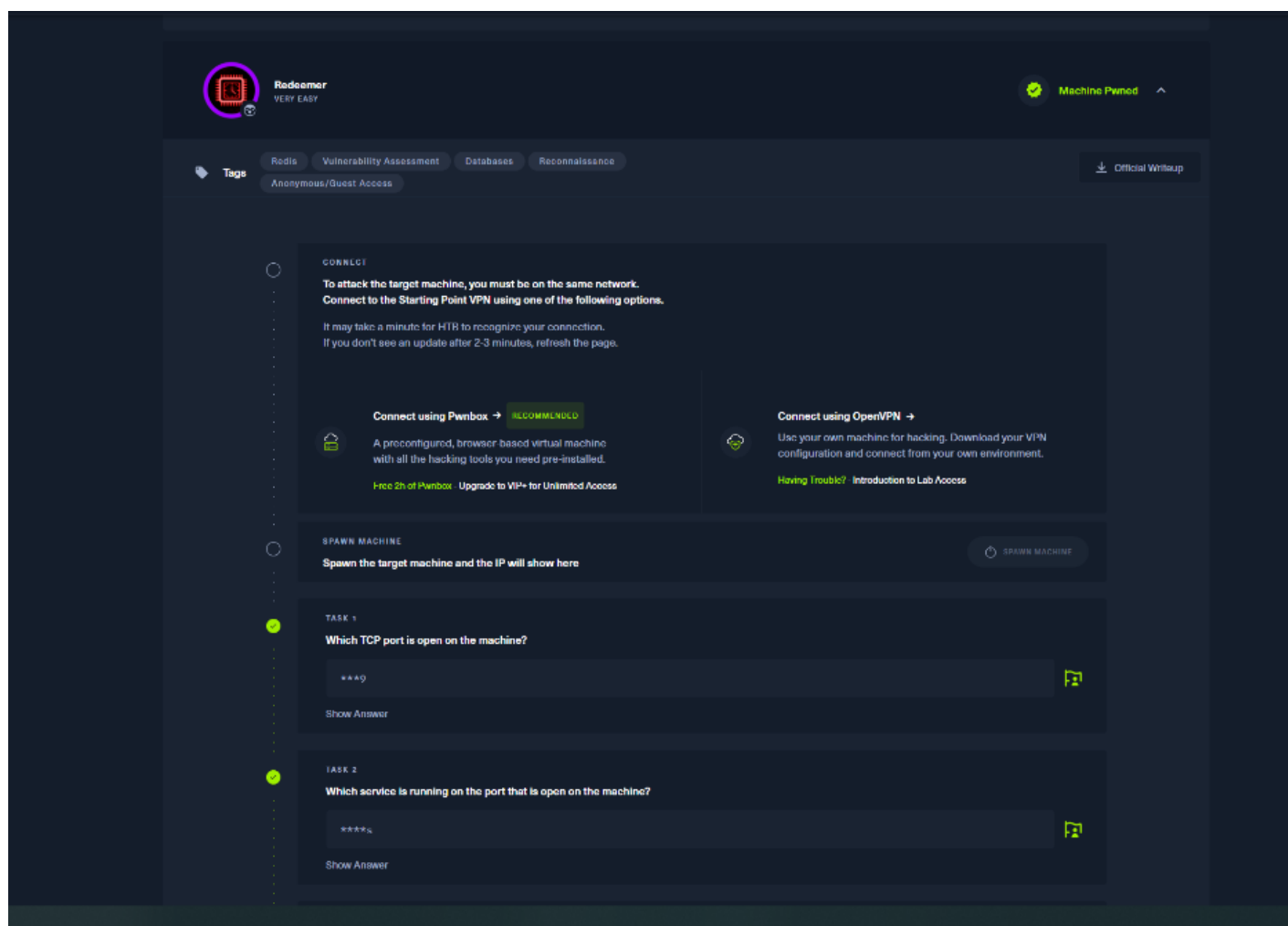
Technical Details:

- Open Ports: 6379 (Redis)
- Service: Redis key-value store
- Vulnerability: Unsecured Redis instance

The **ping** command was used to ensure network connectivity. An **Nmap** scan was performed, which detected that the Redis service was running on **port 6379**.

Unauthenticated access to the Redis instance was identified. Using the **KEYS *** command, all available keys were listed, revealing a key containing the flag. The **GET** command was executed to extract the flag, successfully concluding the test.

Screenshot of the machine.



Screenshot showing the retrieved flag:

```
Parrot Terminal
File Edit View Search Terminal Help
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-qfra2sint3]-[~]
[*]$ nmap -sS -p 1-10000 -sV -v 10.129.94.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-10 01:47 CST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 01:47
Scanning 10.129.94.109 [4 ports]
Completed Ping Scan at 01:47, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:47
Completed Parallel DNS resolution of 1 host. at 01:47, 0.00s elapsed
Initiating SYN Stealth Scan at 01:47
Scanning 10.129.94.109 [10000 ports]
Discovered open port 6379/tcp on 10.129.94.109
Completed SYN Stealth Scan at 01:47, 1.19s elapsed (10000 total ports)
Initiating Service scan at 01:47
Scanning 1 service on 10.129.94.109
Completed Service scan at 01:47, 6.24s elapsed (1 service on 1 host)
NSE: Script scanning 10.129.94.109.
Initiating NSE at 01:47
Completed NSE at 01:47, 0.00s elapsed
Initiating NSE at 01:47
Completed NSE at 01:47, 0.00s elapsed
Nmap scan report for 10.129.94.109
Host is up (0.0087s latency).
Not shown: 9999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
6379/tcp  open  redis    Redis key-value store 5.0.7

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.70 seconds
Raw packets sent: 10004 (440.152KB) | Rcvd: 10002 (400.128KB)
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-qfra2sint3]-[~]
[*]$ redis-cli -v
redis-cli 7.0.15
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-qfra2sint3]-[~]
[*]$ redis-cli -h 10.129.94.109
10.129.94.109:6379> info
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924
redis_mode:standalone
os:Linux 5.4.0-77-generic x86_64
arch_bits:64
multiplexing_api:epoll
```

