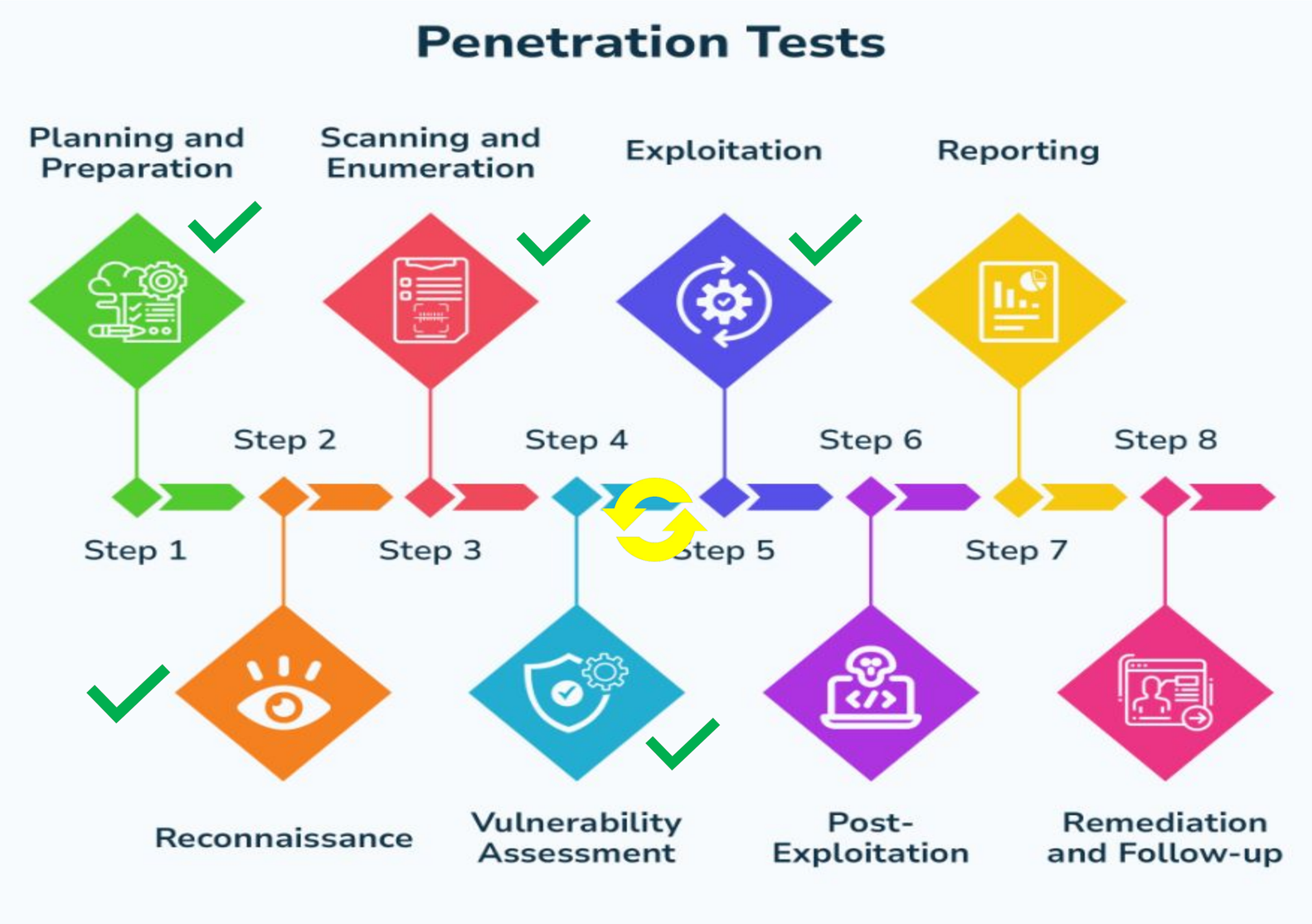
THE BRIDGE

CYBER SECURITY

Post-Explotación: Persistencia Linux

Fases del Pentest



https://www.stationx.net/penetration-testing-steps/

TACTICS

Enterprise

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- **Persistence**
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

Home > Tactics > Enterprise > Persistence

Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

ID: TA0003
Created: 17 October 2018
Last Modified: 19 July 2019

Version Permalink

Techniques

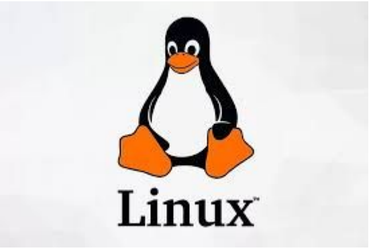
Techniques: 20

ID	Name	Description
T1098	Account Manipulation	Adversaries may manipulate accounts to maintain and/or elevate access to victim systems. Account manipulation may consist of any action that preserves or modifies adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials.

Persistencia. Linux

```
Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09      excellent  No     APT Package Manager Persistence
   1  exploit/linux/local/autostart_persistence           2006-02-13       excellent  No     Autostart Desktop Item Persistence
   2  exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profile Persistence
   3  exploit/linux/local/cron_persistence                1979-07-01       excellent  No     Cron Persistence
   4  post/linux/manage/sshkey_persistence                                 excellent  No     SSH Key Persistence
   5  exploit/linux/local/service_persistence             1983-01-01       excellent  No     Service Persistence
   6  exploit/linux/local/yum_package_manager_persistence  2003-12-17      excellent  No     Yum Package Manager Persistence
   7  exploit/linux/local/rc_local_persistence            1980-10-01       excellent  No     rc.local Persistence
```



.004	SSH Authorized Keys	Adversaries may modify the SSH `authorized_keys` file to maintain persistence on a victim host. Linux distributions and macOS commonly use key-based authentication to secure the authentication process of SSH sessions for remote management. The `authorized_keys` file in SSH specifies the SSH keys that can be used for logging into the user account for which the file is configured. This file is usually found in the user's home directory under `<user-home>/.ssh/authorized_keys`. Users may edit the system's SSH config file to modify the directives PubkeyAuthentication and RSAAuthentication to the value "yes" to ensure public key and RSA authentication are enabled. The SSH config file is usually located under `/etc/ssh/sshd_config`.

.003	Cron	Adversaries may abuse the `cron` utility to perform task scheduling for initial or recurring execution of malicious code. The `cron` utility is a time-based job scheduler for Unix-like operating systems. The `crontab` file contains the schedule of cron entries to be run and the specified times for execution. Any `crontab` files are stored in operating system-specific file paths.

Persistencia. Linux

Account Manipulation: SSH Authorized Keys

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/new_rsa_key
Your public key has been saved in /home/kali/.ssh/new_rsa_key.pub
The key fingerprint is:
SHA256:fEVJGzKRUiNyZOOFHgJuwmRauEBHqdoPl1iNvn8QCkQ kali@kali
The key's randomart image is:
+---[RSA 2048]----+
|.+Eoo ... *oB++.   |
|o*oo  .=++.=.o   |
|oo+ oo o.o  o    |
| ... oo o..  .    |
|..  = o .S .     |
|. + = .  .       |
|   + . .         |
|    o   .        |
|     ...         |
+----[SHA256]-----+
```

```
root@metasploitable3-ub1404:~# cat /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC0iQ9bYCSahBbNEhY8mMoPNb7X12eEF75gtsc
3SH03pMkWbsfufx54fxtb7yhbWC8fs/h9FxgQiUXLRTFuf7CH5o7OM0h2Sieh+lZxs8S/qDltG9
XPNwiaYbJkfXrB3SGUybudhH1q6CaBndrfq/WjHGVQ8nkuzrDQiiKUBScOisl6bsbLY08+iSmSe
root@metasploitable3-ub1404:~# echo '' > /root/.ssh/authorized_keys
root@metasploitable3-ub1404:~#
```

Persistencia. Linux

Scheduled Task/Job: Cron-Jobs

```
* * * * * comando
| | | | |
| | | | +----- Día de la semana (0 - 7) (Domingo=0 o 7)
| | | +------- Mes (1 - 12)
| | +--------- Día del mes (1 - 31)
| +----------- Hora (0 - 23)
+------------- Minuto (0 - 59)
```


THE
BRIDGE