Lab 2

Password Security Implementation and Testing

Do not use vendor-supplied defaults for system passwords and other security parameters

Summary:

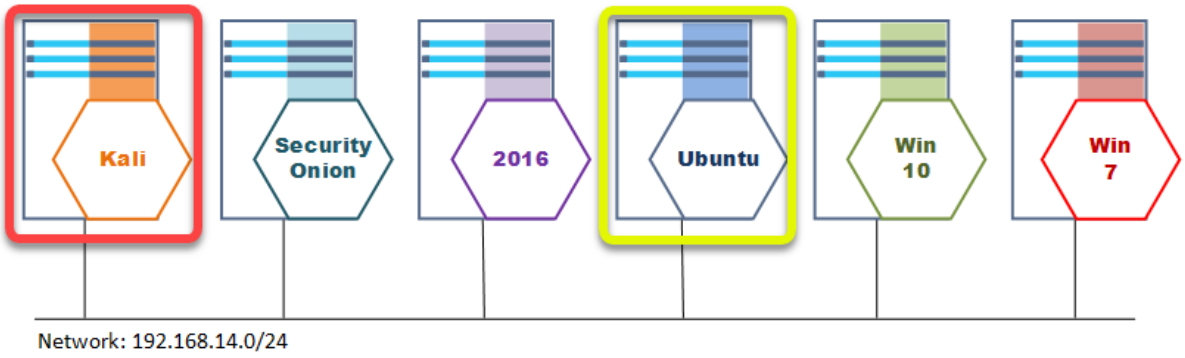
The default settings of many commonly used systems are well known, easily exploitable and often used by criminal hackers to compromise those systems. Vendor-supplied default settings must, therefore, be changed, and unnecessary default accounts disabled or removed before any system is installed on a network. This applies to all default passwords, without exception. If firewalls are correctly implemented according to Requirement 1, they should also comply with Requirement 2.

Lab Setup:

We need a way to ensure that all default credentials for a given product have not been left set to initial install values. We can use a tool called Hydra to test for all known default username:password combinations known for a given system/application. For this particular Exercise we will be auditing the Ubuntu machine but the same type of scripts can be used to audit the windows machines.

PCI_DSS Mapping:

> 2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point -of- sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.)



Audit:

Audit HowTo:

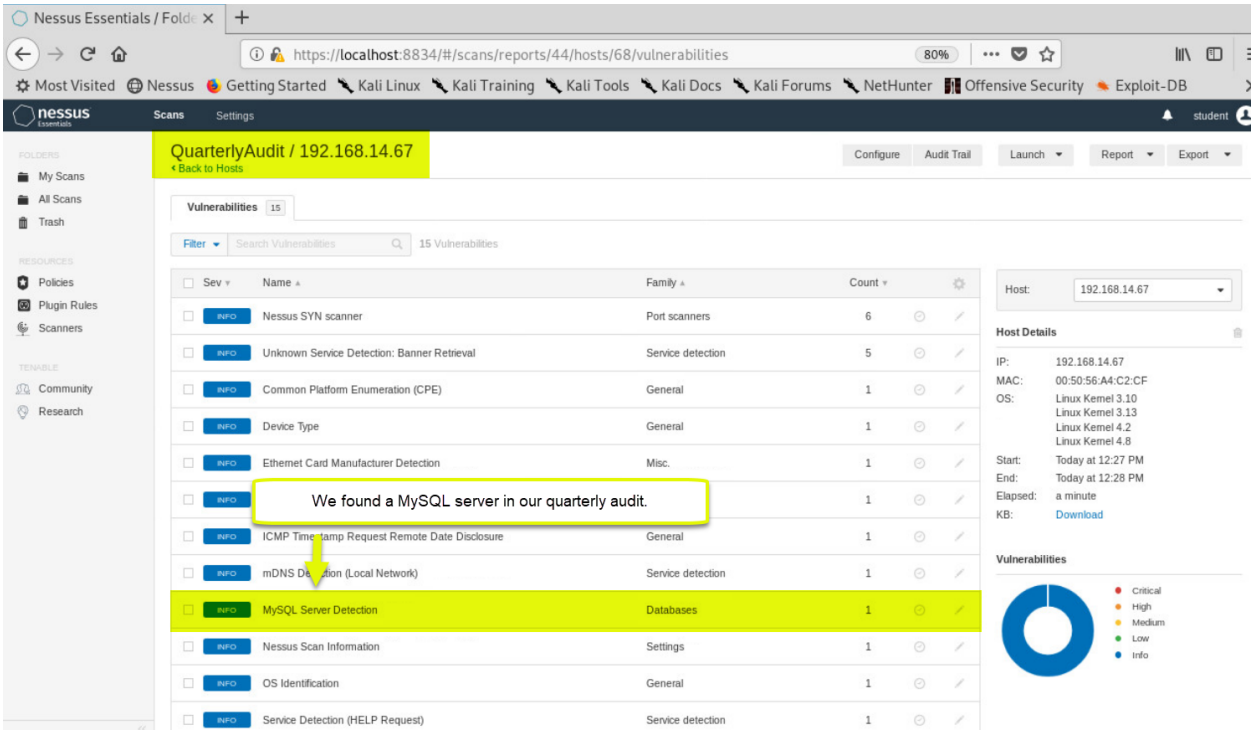
Ubuntu MySQL
Target IP: 192.168.14.67:3306

Finding applications to audit:

Finding applications to audit if fairly easy. We can look at our Quarterly Nessus vulnerability scan to see what applications are available on the network.

Here we find:

- 192.168.14.67
- MySQL Server Database



Testing Default Credentials:

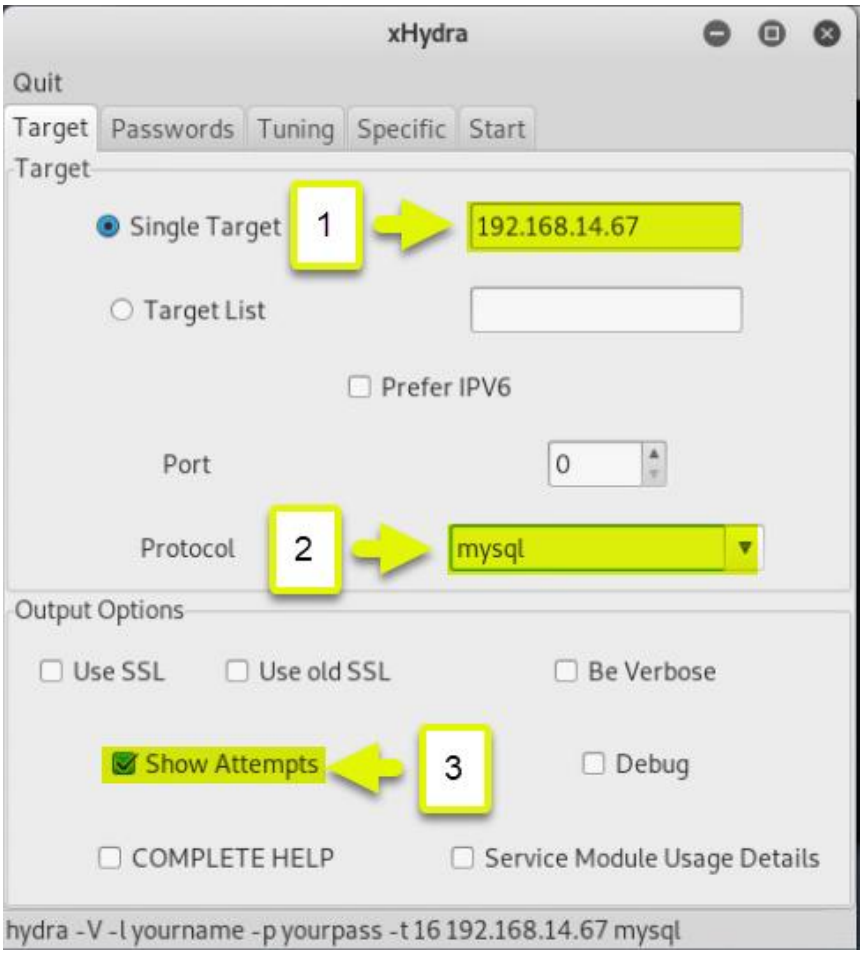
We are going to be using xhydra to test for known default credentials. This is a bit of a manual process as different products have different default username:password combinations. An example of this is that a “D-Link” home access point is going to have a different set of default credentials than a freshly installed POS (Point of Sale) device.

Step 1) Start up the graphical version of Hydra

```
xhydra &
```

Step 2) Set up the target

1. Single Target IP Address = 192.168.14.67
2. Target Protocol = mysql (Note: this will use the default port for the service)
3. Show Attempts (This lets us watch each attempt)



Step 3) Setup your credential list:

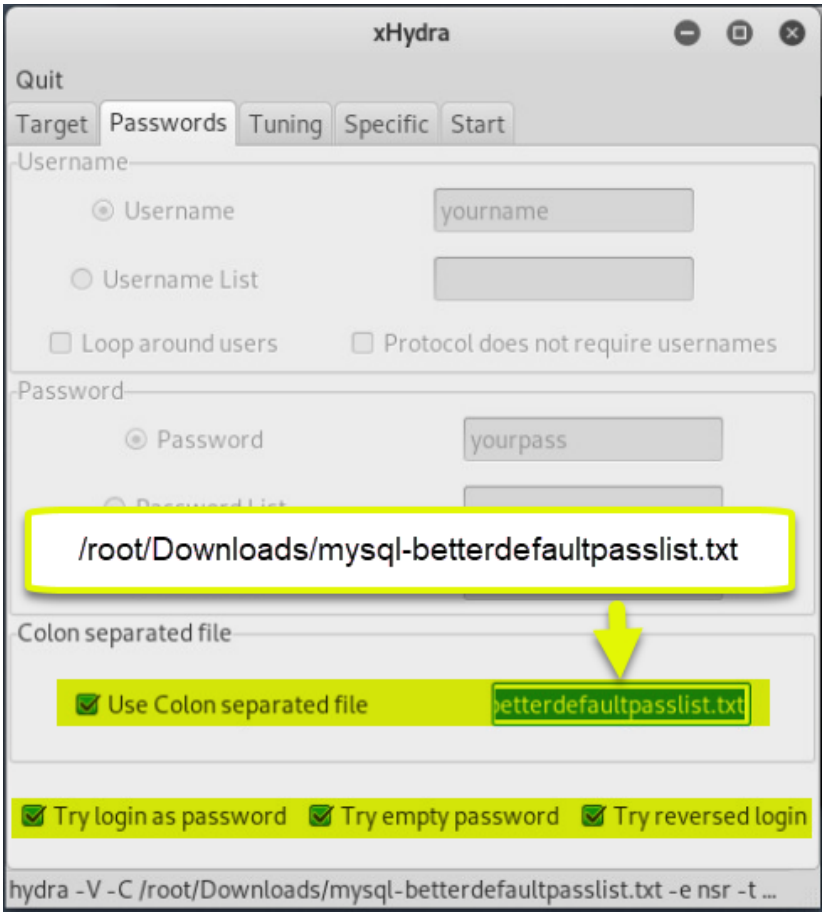
We can do research and find out what the default credentials are for any product we are auditing and build our own list. In this case I just downloaded a list of default credentials for the MySQL server from:
https://github.com/danielmiessler/SecLists/tree/master/Passwords/Default-Credentials

The format of the credentials in this particular file is:

username:password

So we are going to select “Use Colon separated file” and put in the path to our mysql default credentials file. We also always want to:

1. Try login as password
2. Try empty password
3. Try reversed login



Step 4) Run the audit

ToDo:

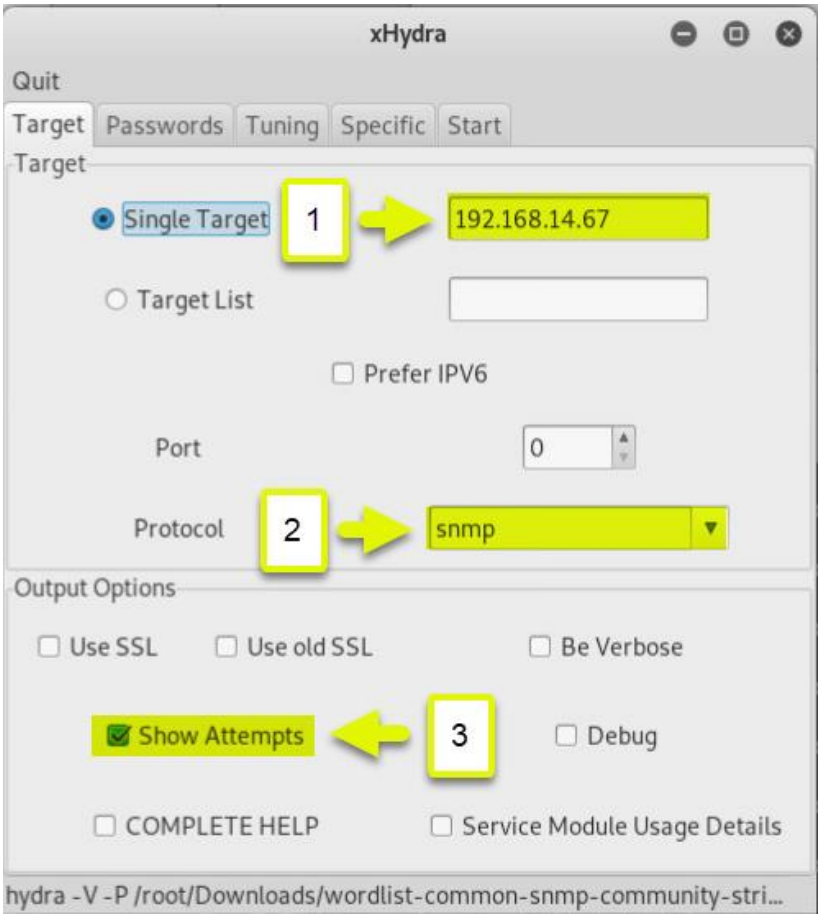
You are going to do the same exercise as the MySQL test only this time we are checking if the “SNMP Community string” was left as a known default. Note: There are a few settings that it is easy to miss causing your test to fail, so we are doing this “ToDo” as a bit of a walk through.

Step 1) Start up the graphical version of Hydra

```
xhydra &
```

Step 2) Set up the target

1. Single Target IP Address = 192.168.14.67
2. Target Protocol = snmp (Note: this will use the default port for the service)
3. Show Attempts (This lets us watch each attempt)



Step 3) Setup your credential list:

We can do research and find out what the default credentials are for any product we are auditing and build our own list. In this case I just downloaded a list of default snmp community strings from:
https://raw.githubusercontent.com/fuzzdb-project/fuzzdb/master/wordlists-misc/wordlist-common-snmp-community-strings.txt

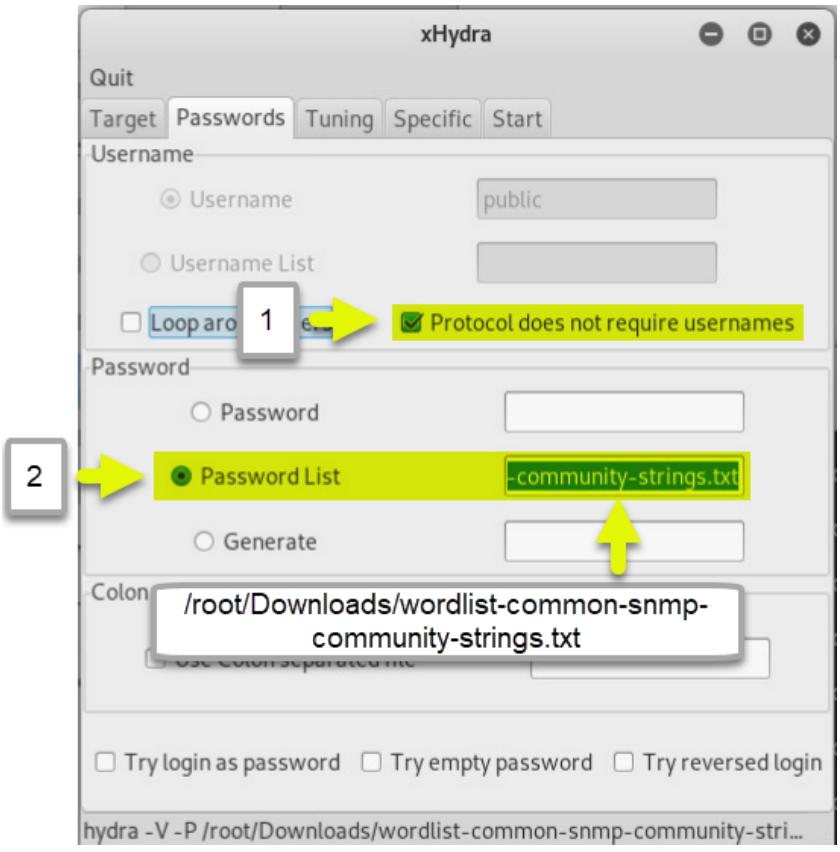
The format of the credentials in this particular file is:

password

Note: We only need the “password” credential for this (being used as a community string), not a username

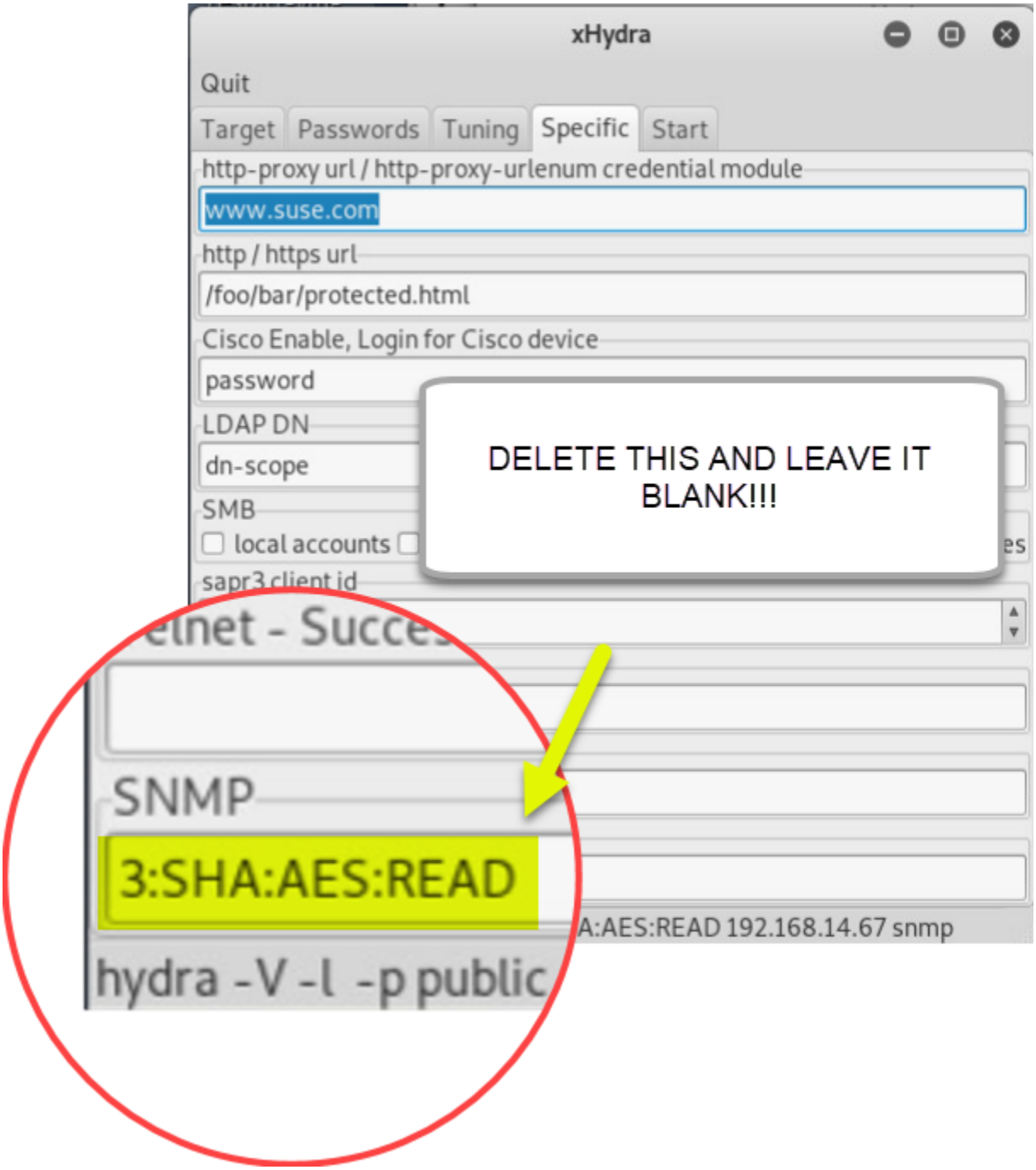
So we are going to select “Use Colon separated file” and put in the path to our mysql default credentials file. We also always want to:

1. “Protocol does not require usernames” MUST BE CHECKED
2. Set the path to our list of community strings to try



Step 4) Set to test SNMPv2c:

By default xHydra is set up to try “SNMPv3”. The server default is using “SNMPv2c”. We need to clear the SNMP field here for our test to work.



Step 4) Run the test:

Questions:

Were there any default SNMP community strings used on the target?

_____

References:

Default Passwords (CERT)
https://cirt.net/passwords

Default Credentials:
https://github.com/danielmiessler/SecLists/tree/master/Passwords/Default-Credentials

6 Ways to Hack SNMP Password:
https://www.hackingarticles.in/6-ways-to-hack-snmp-password/