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.

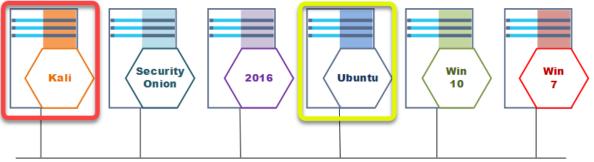
| Summary:  | 1  |
|---|----|
| Lab Setup:                                      | 2  |
| PCI_DSS Mapping:                                | 2  |
| Audit HowTo:                                    | 3  |
| Finding applications to audit:                  | 3  |
| Testing Default Credentials:                    | 4  |
| Step 1) Start up the graphical version of Hydra | 4  |
| Step 2) Set up the target                       | 4  |
| Step 3) Setup your credential list:             | 5  |
| Step 4) Run the audit                           | 6  |
| ToDo:   | 7  |
| Step 1) Start up the graphical version of Hydra | 7  |
| Step 2) Set up the target                       | 7  |
| Step 3) Setup your credential list:             | 8  |
| Step 4) Set to test SNMPv2c:                    | 9  |
| Step 4) Run the test:                           | 10 |
| Questions:                                      | 10 |
| References:                                     | 11 |

## 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.)



Network: 192.168.14.0/24

## 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

| O Nessus Essentia                                  |   |                                 |             |       |              | - •   |                | -       |
|--|---|---------------------------------|-------------|-------|--------------|---|----------------|---------|
| ←)→ ୯ û  | (i) A https://localhost:8834/#/scans/reports/44/h   |                                 |             | 80    |              |   |                |         |
| 🌣 Most Visited 🧲                                   | 🕽 Nessus   🍯 Getting Started 🥆 Kali Linux 🦄 Kali Training 🦄 Ka  | ili Tools 🌂 Kali Docs 🌂 Kali Fo | rums 🌂 NetH | unter | Offensiv     | ve Security 🔺 Ex  | oloit-DB       |         |
|  | Scans Settings  |                                 |             |       |              |   | ٠              | student |
| FOLDERS  | QuarterlyAudit / 192.168.14.67<br><back hosts<="" td="" to=""><td></td><td>Configure</td><td>Auc</td><td>dit Trail La</td><td>aunch - Report</td><td>▼ Exp</td><td>port 💌</td></back> |                                 | Configure   | Auc   | dit Trail La | aunch - Report  | ▼ Exp          | port 💌  |
| <ul> <li>All Scans</li> <li>Trash</li> </ul>       | Vulnerabilities 15  |                                 |             |       |              |   |                |         |
|  | Filter  Search Vulnerabilities Q, 15 Vulnerabilities  |                                 |             |       |              |   |                |         |
| Policies   | Sev v Name *  | Family *                        | Count *     |       | но           | ost: 192.168.14   | .67            | •       |
| <ul> <li>Plugin Rules</li> <li>Scanners</li> </ul> | Nessus SYN scanner  | Port scanners                   |             | 6 🥝   |              | t Details   | Is             |         |
|  | Unknown Service Detection: Banner Retrieval   | Service detection               | 5           |       | IP:          | 192.168.14.67   |                |         |
| n Community  | Common Platform Enumeration (CPE)   | General                         | 1           |       | MAC<br>OS:   | Linux Kernel 3.10   | )              |         |
| Research   | Device Type   | General                         | 1           |       | ×            | Linux Kernel 3.1:<br>Linux Kernel 4.2<br>Linux Kernel 4.8 | 5              |         |
|  | Ethernet Card Manufacturer Detection  | Misc.                           | 1           |       | Start        |   |                |         |
|  | We found a MySQL server in our quart  | erly audit.                     | 1           |       | Elap:<br>KB: |   |                |         |
|  | ICMP Time_tamp Request Remote Date Disclosure   | General                         | 1           |       | 2            |   |                |         |
|  | mDNS Da ztion (Local Network)   | Service detection               | 1           |       | Vuln         | nerabilities  | Critical       |         |
|  | MySQL Server Detection  | Databases                       | 1           |       | <u> </u>     |   | High<br>Medium |         |
|  | Nessus Scan Information   | Settings                        | 1           |       | 1            |   | Low            |         |
|  | OS Identification   | General                         | 1           |       | 7            |   |                |         |
|  | Service Detection (HELP Request)  | Service detection               | 1           |       | 1            |   |                |         |

### **Testing Default Credentials:**

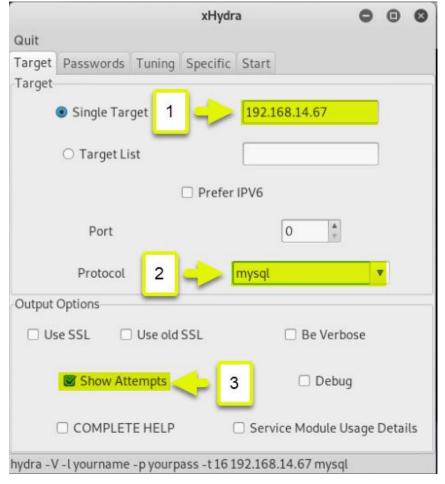
We are going to be using xhydra to test for known default credentials. This is a bit of a manual process as different products have different default username:password combinations. An example of this is that a "D-Link" home access point is going to have a different set of default credentials than a 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

|          |                 |          | xHydr     | а             |            | • •        | 0   |
|----------|-----------------|----------|-----------|---------------|------------|------------|-----|
| Quit     |                 |          |           |               |            |            |     |
| Target   | Passwords       | Tuning   | Specific  | Start         |            |            |     |
| Userna   | me              |          |           |               |            |            |     |
| (        | Username        |          |           | yourname      |            |            |     |
| 0        | Username Li     | st       |           |               |            |            |     |
|          | oop around u    | sers     | Prote     | ocol does not | require u  | sernames   | 2   |
| Passwo   | ord             |          |           |               |            |            |     |
|          | Passwo          | ord      |           | yourpass      |            |            |     |
|          | O Decouver      | Ulint    |           |               |            |            |     |
| /r       | oot/Down        | oads/n   | nysql-b   | etterdefau    | ıltpassli  | st.txt     |     |
| Colon s  | eparated file   |          |           |               | •          |            |     |
|          | l Use Colon s   | eparated | file      | etterd        | efaultpass | ilist.txt  |     |
| Try      | login as passv  | word 👿   | Try empt  | y password    | 🕑 Try re   | eversed lo | gin |
| hydra -V | / - C /root/Dov | wnloads/ | mysql-bet | tterdefaultpa | sslist.txt | -e nsr -t  |     |

Step 4) Run the audit

|  |  | xHydra      | • •          | 8 |
|--|--|-------------|--------------|---|
| Quit   |  |             |              |   |
| Target Passwords Tuning Specific Start       |  |             |              |   |
| Output                                       |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
| Click start to kick off the audit            |  |             |              |   |
| Click start to kick off the addit            |  |             |              |   |
|  |  |             |              |   |
|  |  |             |              |   |
| V  |  |             |              |   |
| Start  | Stop                                       | Save Output | Clear Output |   |
| hydra -V -C /root/Downloads/mysql-betterdefa | ultpasslist.txt -e nsr -t 16 192.168.14.67 | mysql       |              |   |

### ToDo:

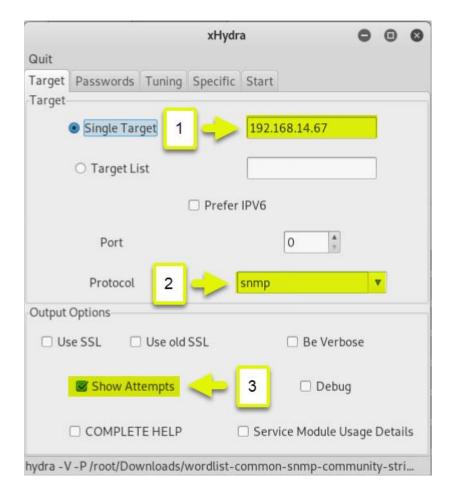
You are going to do the same exercise as the MySQL test only this time we are checking if the "SNMP Community string" was left as a known default. Note: There are a few settings that it is easy to miss causing your test to fail, so we are doing this "ToDo" as a bit of a walk through.

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/wordlistcommon-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

|           |                |           | xHydr      | а                      | 0             | •       | 0    |
|-----------|----------------|-----------|------------|------------------------|---------------|---------|------|
| Quit      |                |           |            |                        |               |         |      |
| Target    | Passwords      | Tuning    | Specific   | Start                  |               |         |      |
| Userna    | me             |           |            |                        |               |         |      |
|           | Osername       |           |            | public                 |               |         |      |
|           | Username Li    |           | Prote      | ocol does not          | require user  | mame    | c    |
| Passwo    | -              | e         | e Prot     | ocor does not          | require user  | name    | 2    |
| rasswo    | O Passwo       | ord       |            |                        |               |         |      |
|           | Password       | List      |            | -commun                | ity-strings.t | xt      |      |
|           | ⊖ Genera       | ite       |            |                        | •             |         |      |
| Colon     | /root/Dov      |           |            | st-commo<br>trings.txt | n-snmp-       |         |      |
|           |                | paratea   | me         |                        |               | _       |      |
| 🗆 Try     | login as passv | word 🗆    | Try empt   | y password             | Try reve      | rsedlo  | ogir |
| hydra - V | /-P/root/Dov   | vnloads/v | wordlist-o | ommon-snn              | np-communi    | ity-str | i    |

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.

|             |            |                 |              | xHydra    | a             |          |         | •     | •  | 8  |
|-------------|------------|-----------------|--------------|-----------|---------------|----------|---------|-------|----|----|
|             | Quit       |                 |              |           |               |          |         |       |    |    |
|             | Target     | Passwords       | Tuning       | Specific  | Start         |          |         |       |    |    |
|             |            | oxy url / http- | proxy-urle   | enum cree | dential       | module   | 2       |       |    | _  |
|             | www.s      | use.com         |              |           |               |          |         |       |    |    |
|             | http/ht    |                 |              |           |               |          |         |       |    | _  |
|             |            | r/protected.h   |              |           |               |          |         |       |    |    |
|             |            | nable, Login f  | for Cisco de | evice     |               |          |         |       |    | _  |
|             | passwo     |                 |              |           |               |          |         |       | _  |    |
|             | LDAPD      |                 |              |           |               |          |         |       |    |    |
|             | dn-sco     | pe              | DEL          | ETE T     | HIS /<br>BLAN |          | EAV     |       |    |    |
|             | SMB        | accounts 🗌      |              |           | DLAP          |          |         |       |    |    |
|             | sapr3 cl   |                 |              |           |               |          |         |       |    | es |
|             |            |                 |              |           |               |          |         | _     |    |    |
|             | tor        | SUCCE           |              |           |               |          |         |       |    |    |
| etr         | net -      | Succe           | -            |           |               |          |         |       |    | *  |
| etr         | net -      | Succe           |              |           |               |          |         |       |    |    |
|             | net -      | Succe           |              |           |               |          |         |       |    |    |
|             |            | Succe           |              |           |               |          |         |       |    |    |
| SNN         | ИР         |                 |              |           |               |          |         |       |    |    |
| SNN         | ИР         |                 |              |           |               |          |         |       |    |    |
| SNN         | ИР         | AES:R           |              | A:AES     | :READ         | 192.16   | 58.14.6 | 7 snr | np |    |
| SNN<br>3:SI | MP<br>HA:/ | AES:RI          | EAD          |           | S:READ        | 9 192.16 | 58.14.6 | 7 snr | np |    |
| SNN<br>3:SI | MP<br>HA:/ |                 | EAD          |           | :READ         | ) 192.16 | 58.14.6 | 7 snr | np |    |
| SNN<br>3:SI | MP<br>HA:/ | AES:RI          | EAD          |           | :READ         | 192.16   | 58.14.6 | 7 snr | np |    |
| SNN<br>3:SI | MP<br>HA:/ | AES:RI          | EAD          |           | :READ         | 192.16   | 58.14.6 | 7 snr | np |    |

Step 4) Run the test:

|  | xHydra             | • • •        |
|--|--------------------|--------------|
| Quit   |                    |              |
| Target Passwords Tuning Specific Start                                     |                    |              |
| Output   |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
| Click start to kick off the audit  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
|  |                    |              |
| Start  | Save Output        | Clear Output |
| hydra -V -C /root/Downloads/mysql-betterdefaultpasslist.txt -e nsr -t 16 1 | 92.168.14.67 mysql |              |

### Questions:

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

## References:

# Default Passwords (CERT) <a href="https://cirt.net/passwords">https://cirt.net/passwords</a>

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/