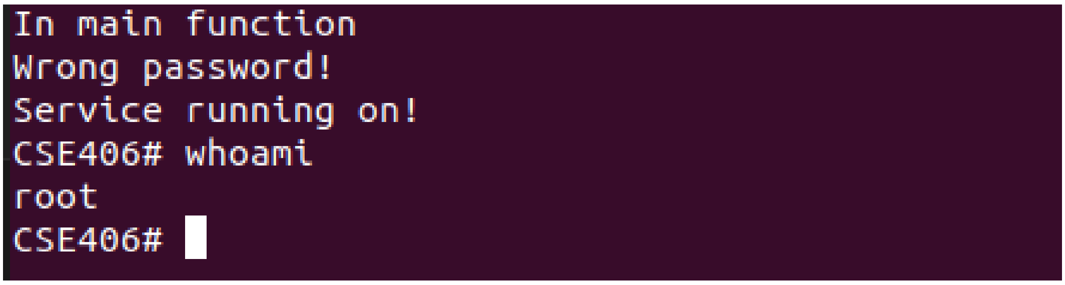
Buffer Overflow Online - A1

Buffer Overflow Attack, CSE 406 January 13, 2024

You are given a vulnerable C program named A1.c. Replace ⟨**PARAM_1**⟩, ⟨**PARAM_2**⟩, ⟨**PARAM_3**⟩ in the source code with the corresponding values of Table-1.

Tasks

- First, you must get the service even though you don't know the password.
- Second, you have to open the shell having root access.
- Prepare payload(s) which will cause the program to run the above tasks.
- Expected Output:



```
In main function
Wrong password!
Service running on!
CSE406# whoami
root
CSE406# █
```

- Ensure you don't change the C program other than the macro parameters values as instructed.
- **You cannot use assembly codes in the exploit py file.**
- **10%** bonus marks if you do the tasks using only the terminal.
- If you have used a cloud VM, make sure to write the public IP of the VM as a comment in the exploit py file.
- Rename your exploit.py file with 19050xx.py and submit it in Moodle.

Table 1: Parameters

ID	PARAM_1	PARAM_2	PARAM_3
1905001	500	700	1500
1905002	485	680	1465
1905003	470	660	1430
1905004	455	640	1395
1905005	440	620	1360
1905006	425	600	1325
1905007	410	580	1290
1905008	395	560	1255
1905009	380	540	1220
1905010	365	520	1185
1905011	350	500	1150
1905012	335	480	1115
1905013	320	460	1080
1905014	305	440	1045
1905015	290	420	1010
1905016	275	400	975
1905017	260	380	940
1905018	245	360	905
1905019	230	340	870
1905020	215	320	835
1905021	200	300	800
1905022	185	280	765
1905023	170	260	730
1905024	155	240	695
1905025	140	220	660
1905026	125	200	625
1905027	110	180	590
1905028	95	160	555
1905029	80	140	520
1905030	65	120	485
Prev 1	50	100	450
Prev 2	35	80	415
Prev 3	20	60	380