2022 CAT-CERT 스터디 보고서

컴퓨터정보공학부 202221168 김지혜

2022.06.01#System \_study-6

1.리눅스 메모리 보호기법에 대해 복습 및 실습

#ASLR

텍스트이(가) 표시된 사진

자동 생성된 설명

실행할때마다 스택의 메모리주소값이 바뀜

(bss와 code는 변하지 않음)

텍스트이(가) 표시된 사진

자동 생성된 설명

“echo 0 > /proc/sys/kernel/randomize\_va\_space” 명령어를 통해 ASLR을 해제 시킴

ASLR을 해제시키면 실행할 때마다 스택의 메모리주소값은 변하지 않고 일정함

-> 보안에 더 취약하게 됨

\*echo 1로 할 경우stack, libc 영역의 값만 바뀐다

\*\*echo 2로 실행할 경우 stack,libc,heap영역의 값이 바뀐다.

#DEX

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

“gcc -m32 -o shell\_c shell\_c.c -fno-stack-protector -mpreferred-stack-boundary=2 -z execstack”을 컴파일 했을 때 스택의 실행권한이 있음

텍스트이(가) 표시된 사진

자동 생성된 설명

“gcc -m32 -o shell\_c shell\_c.c -fno-stack-protector -mpreferred-stack-boundary=2”을 컴파일 했을 때 스택의 실행권한이 없다.

->실행권한이 없기 때문에 메모리 영역의 코드가 실행되지 않는다

또한 스택이나 힙영역에서 shell코드 실행을 막아준다.

#CANARY

텍스트이(가) 표시된 사진

자동 생성된 설명실행파일을 오버플로우하도록 실행시키면 EIP가 원래는 0x41414141로 바뀌어야하는데 그렇지 않고 프로세스가 죽어버린다->canary 때문임

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

Canary의 값의 첫바이트가 null인데 null를 채워주고 메모리 값을 출력해줄때 canary값도 출력이 됨

Ebp-0x6c만큼 입력을 받고 우리가 덮으면 안되는 값이 ebp-0x8에 존재하기 때문에 (0x6c-0x8 )-> 100 만큼 채워주고, null값 1바이트를 채워줘야하기 때문에 총 101바이트를 채워줘야함

(A를 101개까지 받아주고 리틀엔디안으로 출력되니 우리가 보기 쉽게 패킹해준다. 그리고 항상 앞에 값은 null이기 때문에 뒤에 랜덤숫자 3byte를 받아준다)

텍스트이(가) 표시된 사진

자동 생성된 설명

Canary의 값이 출력되는 것을 볼 수 있음

텍스트이(가) 표시된 사진

자동 생성된 설명

Canary의 값을 알았으니 먼저 A를 100개 채워주고, canary의 값을 넣어 통과시켜주고, ebp-0x8에 ret가 있으니까 A를 8개 입력해준다. 그리고 원하는 주소를 입력하면 그 주소로 넘어가게 된다.

Shell을 실행해야하니까 canary의 주소로 shell을 입력한다

#PIE

Pie는 코드주소를 랜덤화시킨다

->코드베이스(시작부분)의 주소를 메모리 리그를 통해서 구한다

“Checksec”

-> 보호기법들이 활성화되어있는지 아닌지 확인할 수 있음

2.Bulpae 서버 /home/junior/hack/ASLR 풀이

3.Wargame.catsecurity.net – protection 풀이