**Unix-privesc-check**

성공적으로 exploit에 성공하였더라도 root의 권한이 없으면 제한 사항이 많을 것이다. 따라서 root의 권한을 얻기 위해서 하는 행동을 elevator 혹은 escalator 라고 한다. 그것을 위한 도구가 이 도구로 localhost에 대하여 process, 실행파일 등의 잘못된 설정 혹은 permission을 확인할 수 있다. 쉽게 말해 root를 열 수 있는 tool이나 설정을 찾는데 용이하다고 한다. 사용법의 경우 간단하다.

“Unix-privesc-check { standard | detailed }”

scan 방식에는 standard와 detailed가 있으며 둘의 차이는 속도, scan 대상 등 이름의 차이에서 어느정도 짐작할 수 있는 점들이다. root의 권한을 찾아낼 수 있는 것은 좋은 도구임이 확실하나 하나의 애로사항을 꼽자면 localhost에 대하여만 실행 가능하다는 점이다.

별도로 remote target에 대하여 실행할 수 없기에 해당 target에서 직접 실행해야 하는데 install과 execute의 경우 tmp directory를 사용하여 한다고 해도 설치 과정에 있어서 외부와 통신 혹은 DNS Query에 문제가 있을 경우 어려움이 있다. 외부에서 직접 다운 받는 것이 아닌 Exploit 과정에서 아예 설치까지 하도록 해버리면 좋을 것 같으나 이는 더 공부를 해야할 것 같다.