x90c article.

+---+
| 리눅스 커널 취약점 익스플로잇팅 (exploiting) |

| 엘리트 x90c (leader) |

| x90chacker@gmail.com |

| x90c research 팀. |
+---/

[목 차]

[1. 개요]:

인트로:
   리눅스 커널 취약점 이라고 할 때 NULL Pointer dereference와 메모리 릭, 레이스컨디션 버그,UAF
(use-after-free) 등을 떠올린다. 그 중에서 많이 보고된 NULL Pointer dereference 취약점이 주요한
해커들의 관심 대상 중 하나가 된다. 이유는 이해하기 쉬운 취약점 공격이고 쉽게 동작하기 때문이다.
mmap_min_addr 커널 파라메타 관련 설정에 따라 공격이 가능한 시스템 배포판이 있고 아닌 경우로
나뉘어 진다.

본 학습 보고서를 통해서 해커는 리눅스 커널 취약점 공격에 대한 기본적인 사항을 학습한다.

[1.1 리눅스 커널]:

리눅스 커널은 리눅스 OS 시스템의 핵심 코드를 의미하는데 운영체제가 부팅이 되어서 동작하고
내부적으로 외부적인 소프트웨어를 운영할 수 있겠금 지원하는 소프트웨어를 OS 커널이라고 한다.

따라서 리눅스 커널이라고 하면 리눅스 OS의 코어 시스템 코드를 말하는 것이다.

[1] 레퍼런스:
  https://ko.wikipedia.org/wiki/리눅스_커널
  (참고로 리눅스는 유닉스 계열 OS 이다.)

[2. 공격 가능한 벡터 소개]:

  고전 do_brk 취약점과 같은 버퍼 오버플로우 성향(메모리 커럽션)의 메모리 침범 취약점은 커널 메모리를
오염시키는 방법으로 공격 하는 기법이었고 현재도 패치가 되지 않은 시스템에서는 리눅스 권한을 상승
시키는 EoP 공격이 가능하다. (do_brk 고전 취약점 지금도 공격은 가능함)

  하지만 많은 수의 시스템이 패치된 지금은 후반에 나온 NULL Pointer dererence 익스플로잇이나
레이스 컨디션 또는 COW (Copy on write) 문제를 다룬 Dirty COW 익스플로잇을 사용해 공격하는 것이 더 적합하다고 할 수도 있다. (요즘 공격 코드가 사용되는 추세)

  코드를 받아 공격하는 경우 vs 새로운 취약점을 코드 분석하는 경우 (쉬움과 어려움)

리눅스 커널 공격은 이미 보고된 공격 코드를 내려받아서 공격하는 방법과 취약한 커널 버전의 소스 코드를
직접 내려 받아 분석해서 공격 코드인 제로데이 코드를 구현해 공격하는 방법이 있지만 제로데이 코드
구현은 쉬운 편이 아니다.

  따라서 공격에 성공하는 것이 목적이라면 즉 모의 해킹 목적에서는 공격 코드를 내려받아서 활용하는 것도
괜찮은 방향이라고 할 수 있다. (쉬운 경우는 공개된 공격 코드를 사용하는 것)

[3. 커널 힙 메모리 공격]:

  인접 메모리 오염(adjacent memory) 공격은 리눅스 커널 힙 메모리 공격 기법인데 이것 역시 해커들의
흥미 대상으로 학습할 만한 주제가 된다. 이것은 리눅스 커널 힙 공격이라고 부른다. x90c 도 이 아티클이
공개 되었을 때 매우 관심을 가졌고 특히 커널 아키텍처적인 이해를 포함한다는 점이 흥미로운 대상이
되었다. 학습 대상으로써 흥미진진했기 때문이다. 물론 이 취약점 공격은 힙 공격의 하나이다.
이 부분에 대해서는 phrack.org 사이트의 아티클을 찾아서 레퍼런스해서 학습하는 것을 추천한다.

구글링을 해도 자료는 있지만 프랙 자료가 좀 더 잘 작성된 편이고 도움이 될 것 같다.

[4. 리눅스 커널 리모트 공격과 로컬 공격]:

  대부분은 리눅스 로컬 권한 상승 익스플로잇이고 sgrakkyu 의 sctp_houdini 나 Jullien 의 madwifi 또한
interrupt context 관련 이슈만 리모트 익스플로잇 관련이다. 다라서 로컬 비중이 아주 크다고 할 수 있다.

[5. 최근 공격 코드가 공유되는 레퍼런스 사이트]:

  최근 공격 코드가 공개 된 사이트는 아래 목록 사이트가 있다.

https://github.com/SecWiki/linux-kernel-exploits

대다수의 공격 코드를 수록하고 있다.

참고 하길 바란다.

[6. 리눅스 커널 익스플로잇의 위험]:

리눅스 커널 공격은 대체로 많은 배포판에서 동작하는 공격 코드들이 많이 공개되어 있어서 여러 배포판의 취약한 서버들이 공격 대상이 될 수 있다는 점이다. 또한 커널 취약점이 특히 위험한 것은 보안 패치가 제공되는 기간이 늦어질 수 있다는 점을 꼽을 수 있다.
또한 취약점 특성 상 시스템 취약점에 포함되기 때문에 시스템 전체가 장악된다는 점이 위험이라고 할 수 있다.

이렇게 3 가지 위험 정도를 들 수 있을 것이다. 물론 조금 더 깊은 이해에서는 다른 관점들도 발생할 수 있다.

[7. 리눅스 커널 공격 역사]:

리눅스 커널 공격 역사에 대해서 간략히 알아 보자.

[7.1 리눅스 커널 공격 연구 역사]:

  리눅스 커널 공격은 2004 년도부터 해커들에 의해 연구 되다가 리눅스 커널을 잘 다루는 존 오버하이드와 같은
유명한 연구원에 의해 다뤄지기 시작 했다. 지금은 대 부분의 공격 기법과 마이티게이션에 대한 익스플로잇이
소개되고 다뤄진 편이다.

...

[7.2 현재 공격 기법 경향 예측]:

...

  따라서 새로운 공격 기법이 소개 될 수도 있고 기존의 공격 코드가 활용될 수도 있는 시점이라는 뜻이다.
보안 패치가 되지 않은 서버는 많기 때문에 운영 관리의 특성 상 리눅스 공격 코드는 많이 사용될 수 있다.

  리눅스 커널 공격에 대한 새로운 이해를 바탕으로 새로운 공격이 출현할 수 있기 때문에 리눅스 커널 공격
영역은 해커들에게 있어서 경이로운 대상이 되기도 한다고 볼 수 있다.

UAF 에 대해서는 추가 적인 학습이 필요한 것 같다.

[8. 결론]:

리눅스 커널 공격에 대해서 알아 보았다.

충분하지 않지만 어느정도 내용의 비기술적인 이야기에서부터 기술적인 얘기를 어느 정도 포함해 아티클을
작성 했다. 기본적인 이해를 하는데 도움이 되었길 바란다.

이상.

 레퍼런스

- main reference:
  https://jon.oberheide.org/files/source10-linuxkernel-jonoberheide.pdf

remote exploit ways:
  - sctp_houdini: http://sgrakkyu.antifork.org/sctp_houdini.c
  - madwifi: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6332
  - interrupt context: (skip)

aeb reference:
  https://www.win.tue.nl/~aeb/linux/hh/hh-12.html (introduce linux kernel exploit)

to become a hacker:
  https://wiki.kldp.org/wiki.php/Hacker-HOWTO

20000.

x90c

엘리트 해커.