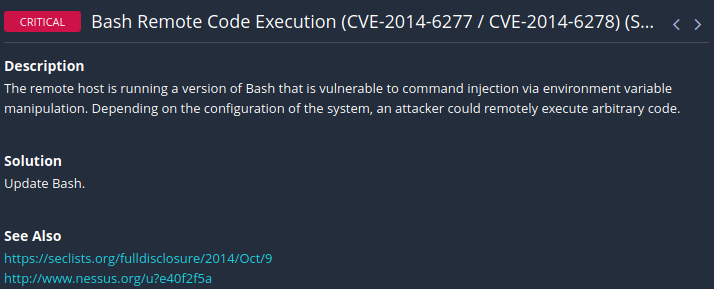
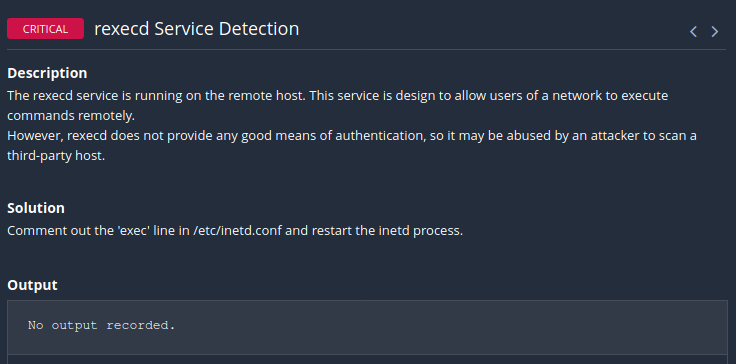
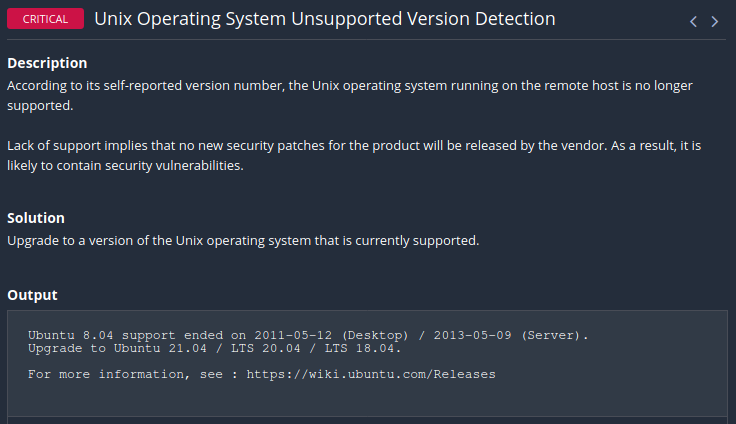
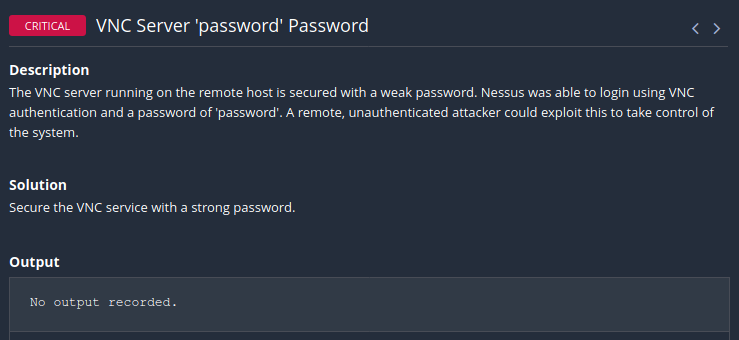
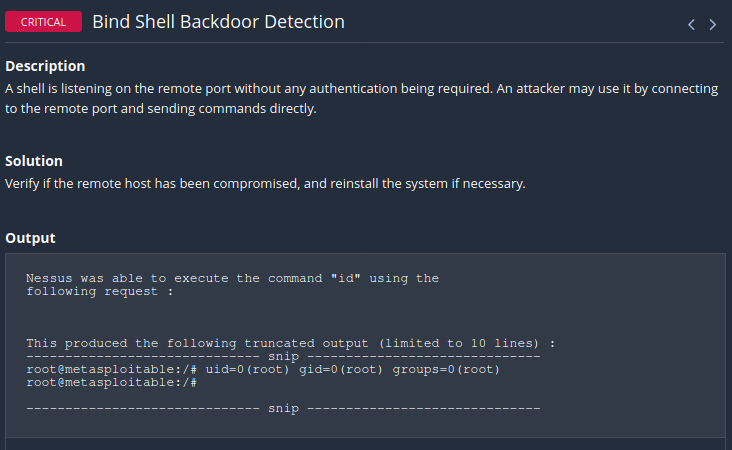
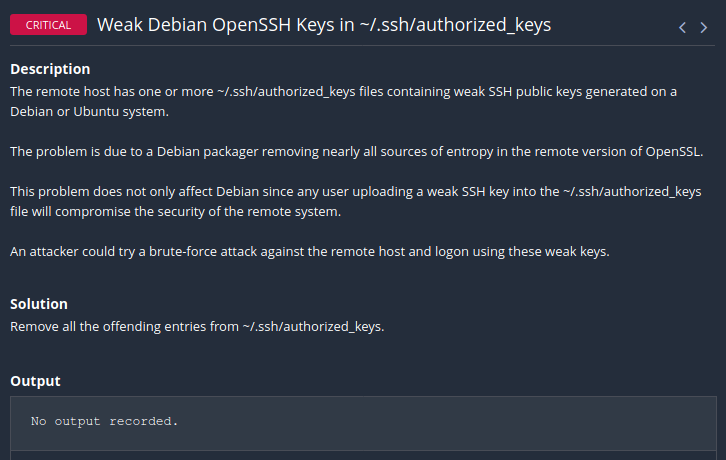
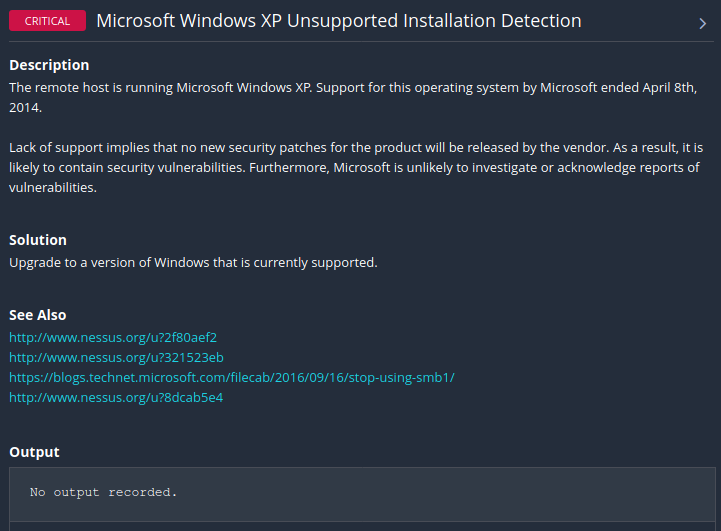
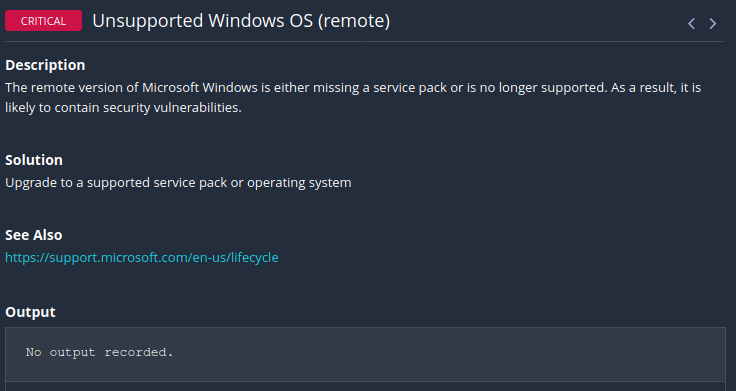
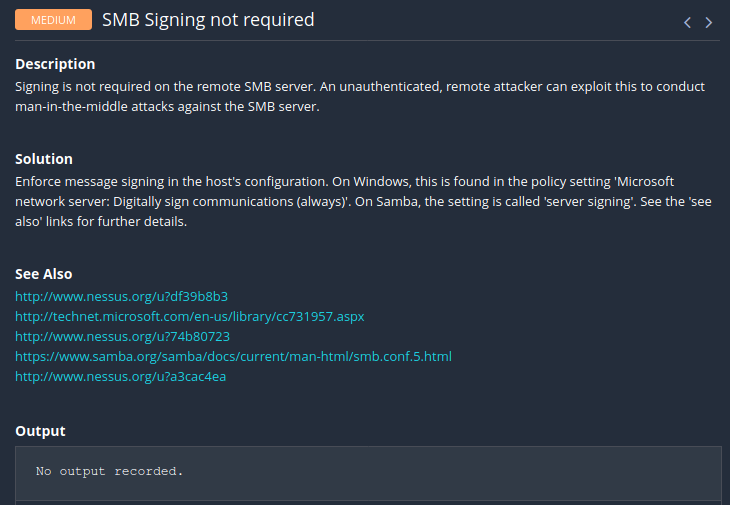
Metasploitable2 취약점

1. Bash Remote Code Execution  
     
   🡪 커멘드 인젝션에 취약한 Bash를 운영하는 원격호스트이다.  
   시스템의 환경에 따라, 공격자는 원격으로 임의의 코드를 실행할 수 있다.
2. NFS Exported Share Information Disclosure  
     
   🡪 원격 서버에서 내보낸 NFS 공유 중 하나 이상을 검색 호스트에서 마운트할 수 있습니다. 공격자는 이를 이용하여 원격 호스트에서 파일을 읽고 쓸 수 있습니다.
3. rexecd Service Detection  
     
   🡪 원격 호스트에서 rexecd 서비스가 실행되고 있습니다. 이 서비스는 네트워크 사용자가 원격으로 명령을 실행할 수 있도록 설계되었습니다.  
   그러나 rexecd는 좋은 인증 수단을 제공하지 않으므로 공격자가 타사 호스트를 검색하는 데 악용될 수 있습니다.
4. Unix Operating System Unsupported Version Detection  
     
   🡪 자체 보고 버전 번호에 따르면 원격 호스트에서 실행 중인 Unix 운영 체제는 더 이상 지원되지 않습니다.  
   지원이 부족하다는 것은 공급업체에서 제품에 대한 새로운 보안 패치를 릴리스하지 않을 것임을 의미합니다. 따라서 보안 취약성이 포함될 수 있습니다.
5. UnrealIRCd Backdoor Detection  
     
   원격 IRC 서버는 공격자가 영향을 받는 호스트에서 임의 코드를 실행할 수 있는 백도어가 있는 UnrealIRCd 버전입니다.
6. VNC Server 'password' Password  
     
   🡪 원격 호스트에서 구동되는 VNC 서버는 약한 패스워드가 설정되어 있다. 암호는 'password'이며, 이를 통해 로그인 및 서비스 제어를 할 수 있어 악용될 수 있다.
7. Bind Shell Backdoor Detection  
     
   🡪 공격자가 원격 포트를 통해 인증 없이 연결을 하고, 커맨드를 직접 전송하여 사용할 수 있다.
8. Weak Debian OpenSSH Keys in ~/.ssh/authorized\_keys  
     
   🡪 원격 호스트에 Debian 또는 Ubuntu 시스템에서 생성된 약한 SSH 공개 키가 포함된 ~.ssh/authorized\_keys 파일이 하나 이상 있습니다.  
     
   이 문제는 원격 버전의 OpenSSL에서 거의 모든 엔트로피 소스를 제거하는 데비안 패커로 인해 발생합니다.  
     
   약한 SSH 키를 ~.ssh/authorized\_keys 파일에 업로드하면 원격 시스템의 보안이 손상되므로 이 문제는 Debian에만 영향을 미치지 않습니다.  
     
   공격자는 원격 호스트에 대해 브루트 포스 공격을 시도하고 이러한 취약한 키를 사용하여 로그온할 수 있습니다.

Window 테의 취약점

1. Microsoft Windows XP Unsupported Installation Detection  
     
   🡪 원격 호스트에서 Microsoft Windows XP를 실행하고 있습니다. Microsoft의 이 운영 체제에 대한 지원은 2014년 4월 8일에 종료되었습니다.  
     
   지원이 부족하다는 것은 공급업체에서 제품에 대한 새로운 보안 패치를 릴리스하지 않을 것임을 의미합니다. 따라서 보안 취약성이 포함될 수 있습니다. 또한 Microsoft는 취약성에 대한 보고서를 조사하거나 인정하지 않습니다
2. Unsupported Windows OS (remote)  
     
   🡪 원격 버전의 Microsoft Windows에 서비스 팩이 없거나 더 이상 지원되지 않습니다. 따라서 보안 취약성이 포함될 수 있습니다.
3. MS08-067: Microsoft Windows Server Service Crafted RPC Request …  
     
   🡪 원격 윈도우 호스트는 부적절한 RPC 요청의 처리로 인해 '서버' 서비스의 원격 코드 실행 취약성의 영향을 받는다. 공격자는 조작된 RPC 요청을 통해 SYSTEM 권한으로 임의의 코드를 실행할 수 있다.  
   🡺 **해당 취약점을 사용해 공격을 진행해 볼 것이다.**
4. MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code …  
     
   🡪 원격 호스트는 SMB의 메모리 손상 취약성의 영향을 받으며 이를 통해 공격자가 원격 호스트에 대해 임의 코드를 실행하거나 서비스 거부를 수행할 수 있습니다.

Window 8.1의 취약점 분석

1. MS16-047: Security Update for SAM and LSAD Remote Protocols …  
     
   원격 윈도우즈 호스트는 원격 프로시저 호출(RPC) 채널을 통한 잘못된 인증 수준 협상으로 인해 SAM(Security Account Manager) 및 LSAD(Local Security Authority) 프로토콜의 권한 상승 취약성의 영향을 받습니다. 클라이언트와 SAM 데이터베이스를 호스팅하는 서버 간의 통신을 가로챌 수 있는 중간 공격자는 이를 이용하여 인증 수준을 강제로 다운그레이드하여 인증된 사용자로 가장하고 SAM 데이터베이스에 액세스할 수 있습니다.
2. SMB Signing not required  
     
   원격 SMB 서버에서는 서명이 필요하지 않습니다. 인증되지 않은 원격 공격자는 이를 이용하여 SMB 서버에 대한 중간자 공격을 수행할 수 있습니다.
3. **[HIGH]MS17-010** : Microsoft Server Message Block 1.0(SMBv1)에는 여러 원격 코드 실행 취약성이 있는데, 이는 특정 요청을 잘못 처리하며 발생하게 된다. 인증되지 않은 원격 공격자는 특수하게 조작된 패킷을 통해 이러한 취약성을 이용하여 임의 코드를 실행할 수 있다.  
   2017/04/14에 Shadow Broker로 알려진 이들이 몇가지 취약점을 공개하였다. ENVERNALBLUE, ENVERCHAMPION, ENVERNALSYERGY가 그것이다. WannaCry / WannaCrypt는 ENVERNALBLUE exploit을 활용한 랜섬웨어 프로그램이며, EvernantRocks는 7가지 EQUATION GROUP 취약점을 활용한 웜이다. Petya는 마이크로소프트 오피스의 취약점인 CVE-2017-0199를 먼저 활용한 뒤 ENVERTBLUE를 통해 전파하는 랜섬웨어 프로그램이다.  
   🡪 **현재는 최신버전으로 다운로드한바 이 취약점은 없어졌다.**