250714

기존 : Pa55word$%^

변경 : Pa55word!@#$%

환경설치

VM, Windows server 2012, .vdi+.vbox

> .vbox 누르면 저장된 환경으로 머신 생성됨.

> .vdi 이름 그대로 두어야 연동됨.

<inbox>

download.virtualbox.org/virtualbox/7.1.4 > 클립보드 및 파일공유 기능 사용

리눅스는 CLI 기반인데에 반해 윈도우는 GUI로 찾아가야함.

문장 작성보다는 데이터 따라가기 및 스크린샷에 집중할 것.

주어진 대상 환경은 AD 설정이 되어있어 ~가이드와 다른 화면으로 확인해야 되는 내용이 있음.

? AD(Active Directory) : 누구냐 넌

? 주어진 결과보고서 양식의 "W-01" 항목의 캡처가 가이드의 내용과 다른데 어떤 차이점이 있는지.

> 확인하는 방법에는 여러 가지가 있고 가이드와는 다른 방식으로 캡처한 것, 차이점?? > 공부 더 하고 싶으면 여러 방향으로 확인해라

? 실무에서도 이런 식으로 캡처 및 결과보고서 작성을 진행하는지 > 놉, 스크립트 돌림

SID(Security ID) : 윈도우즈의 각 사용자 및 그룹에 부여되는 고유한 식별 번호

IIS(Internet Information Services) : 윈도우 운영체제에서 제공하는 웹 서버 SW

> 윈도우에서 Web server, WAS 돌릴 때 사용

> 웹, 네트워크로 발생할 수 있는 많은 취약점에 대해 최소한의 보안 세팅이 필요함.

> Webroot : 웹 설정?데이터? 디렉터리의 최상단 디렉터리를 의미함.

> (W-20)ACL(Access Control List) : 접근이 허가된 주체들과 허가받은 접근 종류들이 기록된 목록.

> CGI(Common Gateway Interface) : IIS에서 동적인 웹페이지를 생성하기 위해 사용됨.

>> 많은 보안 취약점이 발견되었고, 대체 가능한 도구들이 잘 나와있어 최근에는 사용하지 않음.

현재 진단 중인 대상 서버가 가이드 항목의 대상에 포함되어 있지 않으면 진단 대상이 아님. > 표시하고 넘어가면 됨.

가이드에는 설명을 위해 캡처가 많은 경우가 있지만, 결과 보고서는 진단 근거가 포함된 최소한의 캡처로 작성할 것.

전체 보안에서 시스템 보안은 큰 비중을 차지하고 있지는 않음. > 보통 사고의 직접적인 원인이 아님.

윈도우 시스템 진단에 대해서는 항목별 개념 공부도 필요하겠지만 스크립트 짜보고 결과를 결과보고서(excel)에 직접 꽂는 플로우 구성 추천.

윈도우 에서 권한을 이야기할 때는 Everyone 권한(유/무)에 대한 내용이 주를 이룸.

NetBIOS(Network Basic Input/Output System) : 근거리통신망 내에서 파일 등 자원공유 기능을 제공하는 프로그램.

// Summary

취약점 진단 : 취약점진단(guide) + 모의해킹(black,grey,white)

Infra(System) : Windows, Linux, Network, 보안장비, DB 등이 진단 대상

Web Application + Mobile : program, android, ios

수동(캡처 및 내용작성), 반자동(스크립트를 통한 수행 및 텍스트파일출력물 결과보고서에 적용), 자동(진단 솔루션 > 결과보고서 나옴)

250715

예시1. 진단에 사용하고 있는 배치 파일

> 진단 과정 동안 일일히 다시 접속하여 내용을 확인하지 않고, 배치파일 출력물을 활용하여 정보를 확인함.

> 명령어 기반으로 정보를 수집하기 때문에 캡처 등의 이미지는 포함되어 있지 않음.

예시2. 고객사들에게 제공? 혹은 실제 진단에 사용되고 있는 진단가이드

> 가이드내용이 전부 포함되어 있는 것은 물론, 같이 확인 가능한 것은 묶어서 같이 확인함.

> 이에 더해 추가로 확인해야할 사항들에 대해서도 포함되어 있음.

//Summary

1. 3가지 단어(NetBIOS, SNMP, AD)에 대한 개념설명.

2. 계정관리 : 1(Administrator 계정 이름 변경), 2(Guest 계정 비활성화) ,6(관리자 그룹에 최소한의 사용자 포함)

3. 계정 패스워드 관련 정책 및 47(계정 잠금),48(PW복잡성), 49(PW최소길이), 50(PW최대사용기간) ,51(PW최소사용기간) ,52(로그온시배너)

IIS 의 개념, 항목관련 개념

32(최신HOTFIX),31(서비스팩),33(백신프로그램), 70(이벤트로그설정) : 윈도우 특수 설정에 대한 이해