OS 모니터링 시스템 구축

2019. 10. 29

지도교수: 이병천 교수님

팀명: 트론 (이재희, 나경민, 이영상, 이동준, 주영문)

목 차

- 조원 편성
- 주제 선정
- 구 상 도
- 추진 경과
- 개발 환경 및 시스템 개발
- 개발 시스템 운영
- 결론 및 기대효과

조원 편성

조 원	역 할
이재희	진단 프로그램 제작, PPT 작성 (총 괄)
나경민	연동 사이트 제작
이영상	진단 프로그램 제작, 보고서 작성
이동준	연동 사이트 제작
주영문	진단 프로그램 제작

주제 선정 (1/3)

보안 취약점 노리는 사이버 공격 급증...어떻게 대응할까

정보보안 취약점을 노리는 사이버 공격이 날로 증가함에 따라 보안 취약점 진단 중요성이 점점 높아지고 있다.

출처 : 전자신문 (2018.9.11)

한국인터넷진흥원이 7월 말 발표한 2분기 사이버 위협 동향 보고서에 따르면
올해 2분기에 확인된 고위험 보안 취약점은 891개에 달했다.
보안 관리자가 수 많은 취약점을 일일이 찾아 패치하는 데는 한계가 있는 만큼
IT 시스템·애플리케이션·웹 등에 있는 취약점을 자동 진단하는 취약점 분석 솔루션 수요는 더욱 늘어날 전망이다.

시스템 담당자는 취약점 현황 및 조치 결과는 물론 사용자가 원하는 다양한 기준에 부합하는 핵심 위협 정보와 진단 이력을 보다 쉽고 빠르게 파악할 수 있다.
즉 어느 부서가 어떤 보안 위협에 취약한지, 수많은 시스템 중 어떤 IT시스템이 공격 경로로 이용될 가능성이 높은지, 장기적으로 진단이 이뤄지지 않았거나 조치가 미흡했던 부분은 없는지 등을 보다 신속하고 정확하게 인지할 수 있다.

주제 선정 (2/3)

"2018년 한국 보안시장 2조원...전년比 4%↑"
가트너 전망 "2019년 한국 2조2천억원, 세계 1천240억달러"

2017-2019 년 전세계 분야별 보안 지출액 (단위: 백만 달러)

출처 : Zdnet Korea (2018.8.16)

시장 분야	2017	2018	2019
애플리케이션 보안	2,434	2,742	3,003
클라우드 보안	185	304	459
데이터 보안	2,563	3,063	3,524
IAM	8,823	9,768	10,578
인프라 보호	12,583	14,106	15,337
통합 리스크 관리	3,949	4,347	4,712
네트워크 보안 장비	10,911	12,427	13,321
그 외 정보 보안 소프트웨어	1,832	2,079	2,285
보안 서비스	52,315	58,920	64,237
소비자 보안 소프트웨어	5,948	6,395	6,661
총 계	101,544	114,152	124,116

주제 선정 (3/3)

KISA(한국인터넷진흥원) 배포
“주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드”

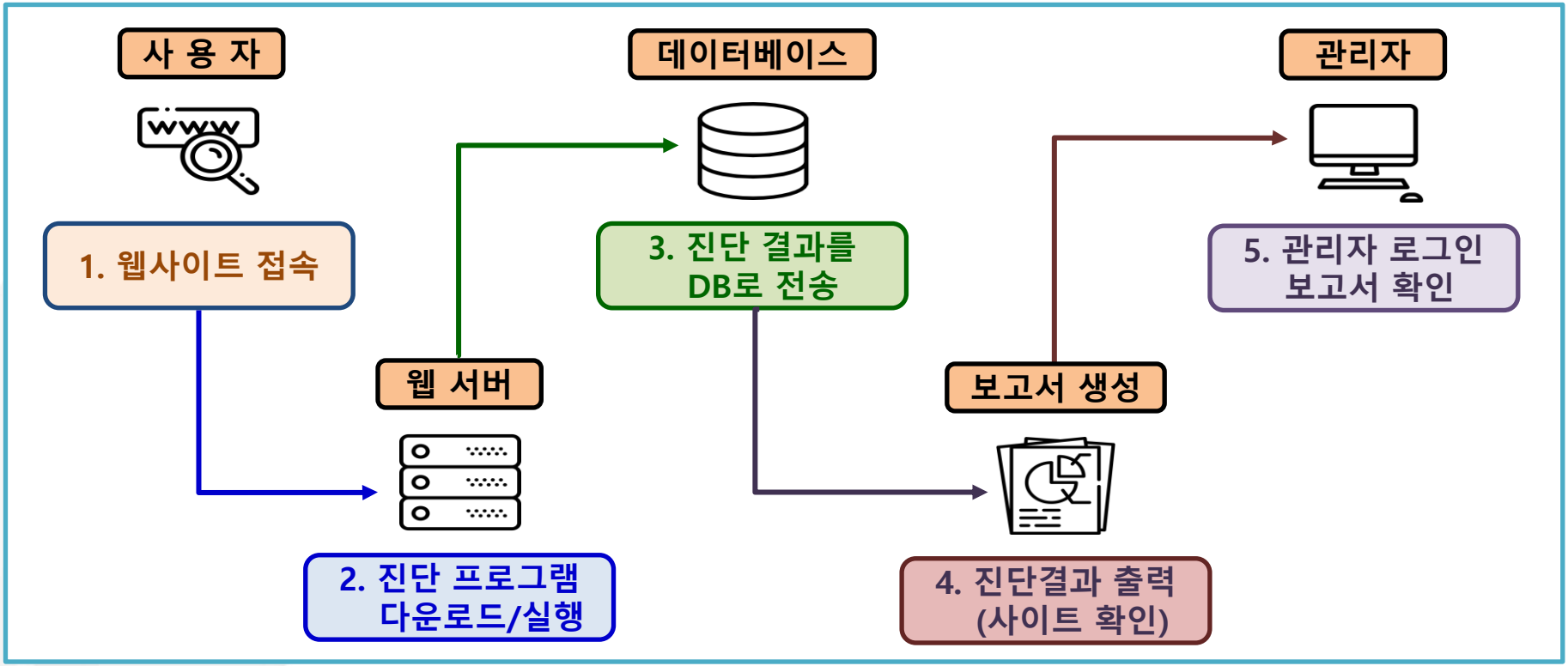
출처 : KISA (2018.6.28)

제목	주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드		
담당자	융합기반보호팀 이성영 ☎ 061-820-1641 ✉		
등록일	2018-06-28	조회수	23859
첨부파일	(한국인터넷진흥원)_주요정보통신기반시설_기술적_취약점_분석_평가_상세_가이드_(2017).pdf		

대분류	소분류	기술안내서 가이드	대상	수준
정보 보호 시스템 안전	정보 보호 시스템 관리	주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드	IT시스템관리자	중급

KISA 취약점 분석 평가 가이드에 기반하여 OS 모니터링 시스템을 개발

구상도


사 용 자
데이터베이스
관리자
1. 웹사이트 접속
3. 진단 결과를
DB로 전송
5. 관리자 로그인
보고서 확인
웹 서버
보고서 생성
2. 진단 프로그램
다운로드/실행
4. 진단결과 출력
(사이트 확인)

추진 경과

추진기간 (2019년) / 대상업무	3월	4월	5월	6월	7월	8월	9월	10월	11월
계획 수립									
자료 조사/분석									
프로그램 제작									
웹 관리패널 작성									
성능시험 및 보완									
종합/보고서 작성									

개발 환경 및 시스템 개발 (1/8)

개발 환경

운영체제

- Windows 10

프로그래밍 언어

- C#
- JSON

웹 환경

- Nginx/PHP 7.2
- MariaDB
- Semantic UI

개발 환경 및 시스템 개발 (2/8)

메인 화면 구현

API

```php
<?php
$conn = mysqli_connect("localhost:3307", "test_db", "asdfasdf", "test_db");
if (mysqli_connect_errno()) {
    echo "MySQL 연결 오류 : " . mysqli_conne
}
echo "DB 접속 OK  ";
?><br/><br/><?php

$select_query = "SELECT idx,Name FROM Host"
$result_set   = mysqli_query($conn, $select
$count        = mysqli_num_rows($result_set
$tmp          = $count + 1;

echo "번호: " . $count . ", 호스트: ", $_GET
", OS: ", $_GET['OS'] . ", Time: ", $_GET['

$sql = mq("INSERT into Host (idx, Name, IP,
```

시각화

```php
$no = 1; // 리스트 번호를 나타냄
while ($row = mysqli_fetch_array($result)) {
    echo "<tr>";
    echo "<td>" . $no . "</td>";
    echo "<td>" . $row['Name'] . "</td>";
    echo "<td>" . $row['IP'] . "</td>";
    echo "<td>" . $row['OS'] . "</td>";
    echo "<td>" . $row['time'] . "</td>";
    echo "</tr>";
    $no++; // idx 를 1씩 증가
}
echo "</tbody></table></center>";
```

시각 정보 제공, 누적 경고 시스템 등 취약점 진단 메뉴 등을 설정

개발 환경 및 시스템 개발 (3/8)

PC 정보 획득

운영체제 정보 획득

```
internal string OSName()
{
    string result = "Not found!";
    ConnectionOptions options = new ConnectionOptions();
    options.Impersonation = ImpersonationLevel.Impersonate;
    ManagementScope scope = new ManagementScope("/root/cimv2", options);
    scope.Connect();
    ObjectQuery query = new ObjectQuery("Select Caption From Win32_OperatingSystem");
    ManagementObjectSearcher search = new ManagementObjectSearcher(scope, query);
    ManagementObjectCollection queryCollection = search.Get();
    foreach (ManagementObject o in queryCollection)
    {
        result = o["Caption"].ToString();
        if (Environment.Is64BitOperatingSystem)
```

※ 캡슐화: 클래스 내부 접근만 가능한 Internal으로 구현 (보안상 이점)

분석 대상 PC를 확인/관리하는데 필수적인 정보를 획득

개발 환경 및 시스템 개발 (4/8)

서비스 진단

위험서비스 확인

```
ListViewItem XServiceList = new ListViewItem();
XServiceList.Text = service.DisplayName;
RegistryKey regKey1 = Registry.LocalMachine.OpenSubKey("SYSTEM\\CurrentControlSet\\services\\" + service.ServiceName);
string StartType = Convert.ToString(regKey1.GetValue("Start"));
// (StartType == 2, 3) 0: 부탕, 1: 시스템, 2: 자동, 3: 수동, 4: 사용 안함
int ServiceStatus = Convert.ToInt32(service.Status);
// (ServiceStatus == 0) 0: 실행 중, 1: 일시 중지 중, 2: 시작 보류 중, 3: 일시 중지 보류 중, 4: 일시 중지 후 서비스 시작 (대기
if (StartType == "2" || (StartType == "3") && (ServiceStatus == 0))
{
    if (StartType == "0") StartType = "부팅 시, 자동 시작";
    else if (StartType == "1") StartType = "시스템";
```

보안에 위험한 서비스가 구동 중인지 확인 ⇨ 취약 서비스 대응

개발 환경 및 시스템 개발 (5/8)

게시판 운영

게시글 작성

```
            <div id="write_area">
            <form class="ui form" action="write_ok.php" method="post" enctype="multipa
<div class="field">
  <label>제목:</label>
  <input type="text" name="title" id ="utitle" rows="1" cols="55" placeholder="제목">
</div>
                    <div class="wi_line"></div>


                    <div id="in_content">
                        <textarea name="content" id="ucontent"></textarea>
                        <!-- 여기서 required는 반드시써야한다는 의미입니다 -->
                        <script>
                        // 3. CKEditor5를 생성할 textarea 지정
                          ClassicEditor
                          .create( document.querySelector( '#ucontent' ) )

                          .catch( error => {
                            console.error( error );
```

취약점 진단 결과 등을 공지하고 위협요인 정보 등을 안내

개발 환경 및 시스템 개발 (6/8)

보안요소 점검

메신저 설치 확인

```
internal bool Messenger(int check)
{
    var drive = Path.GetPathRoot(Environment.SystemDirectory);
    bool installed = false; string test;
    if (check == 0)
    { // Kakaotalk Check
        test = Convert.ToString(Registry.GetValue(@"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft" +
               @"\Windows\CurrentVersion\Uninstall\KakaoTalk", "UninstallString", ""));
        if (File.Exists(test)) return true;
    }
    else if (check == 1)
    { // Line Check
        test = Convert.ToString(Registry.GetValue(@"HKEY_CURRENT_USER\Software\Microsoft" +
               @"\Windows\CurrentVersion\Uninstall\LINE", "UninstallString", ""));
```

메신저 소프트웨어들의 설치 유무를 점검

개발 환경 및 시스템 개발 (7/8)

보안요소 점검(1/2)

화면보호기 확인

```
// 화면 보호기 상태 확인
참조 1개
internal string ScreenSaver()
{
    string screensaver;
    RegistryKey reg = Registry.CurrentUser.OpenSubKey(@"Control Panel\Desktop", true);
    if (reg != null)
    {
        Object val = reg.GetValue("ScreenSaveActive");
        screensaver = Convert.ToString(val);
        Object ssval1 = reg.GetValue("ScreenSaveTimeOut");
        Object ssval2 = reg.GetValue("ScreenSaverIsSecure");
        if (val != null)
```

화면보호기 설정이 안전하게 되어 있는지 확인

개발 환경 및 시스템 개발 (8/8)

보안요소 점검(2/2)

```
internal void CVECheckRun(ListView lvw)
{
    var startInf
    {
        FileName
        Argument
        UseShell
        CreateNo
    };
    Process.Star
```

CVE 취약점

CVE: 소프트웨어의 보안 취약점을 가리키는 표기법 [미국 국립 표준 기술연구소(NIST) 지정]

CVE 정보 확인

Product	ID	Lisk Score
adobe_air 32.0.0.125	CVE-2013-0650	10
adobe_air 32.0.0.125	CVE-2013-0646	10
adobe_air 32.0.0.125	CVE-2013-1375	10
adobe_air 32.0.0.125	CVE-2013-1371	10
adobe_air 32.0.0.125	CVE-2010-2214	9.3
adobe_air 32.0.0.125	CVE-2010-2216	9.3
adobe_air 32.0.0.125	CVE-2010-2213	9.3
adobe_air 32.0.0.125	CVE-2010-0209	9.3
adobe_air 32.0.0.125	CVE-2010-2215	4.3

Vulmon(Vulnerability Intelligence Search Engine) : CVE 취약점을 검출하는 검색엔진

Vulmon의 개발 스크립트에 접속하여 정보를 추출하는 인터페이스 제작

개발 시스템 운영 (1/5)

메인 화면

SW 중심으로 보안 취약점을 자동진단/모니터링하는 시스템 운영

개발 시스템 운영 (2/5)

로그인

로그인을 하면 취약점 진단 서비스를 제공받으며 시스템 사용이 가능

개발 시스템 운영 (3/5)

진단시스템 실행

대상 PC에서 진단시스템 실행 ⇨ 웹 업로드 ⇨ 진단 결과 확인

개발 시스템 운영 (4/5)

진단 PC 목록

수집 내역

Idx	Name	IP	Time	OS
7	DESKTOP-C66KL2I	14.42.86.31	2019-10-22 14:43:59	Microsoft Windows 10 Home 64비트
6	DESKTOP-25ATM5L	14.42.86.31	2019-10-22 14:39:06	Microsoft Windows 10 Pro 64비트
5	DESKTOP-25ATM5L	14.42.86.31	2019-10-22 14:29:45	Microsoft Windows 10 Pro 64비트
4	DESKTOP-C66KL2I	14.42.86.31	2019-10-22 14:29:14	Microsoft Windows 10 Home 64비트
3	DESKTOP-C66KL2I	14.42.86.31	2019년 10월 22일 14시 23분 50초	Microsoft Windows 10 Home 64비트
2	DESKTOP-25ATM5L	14.42.86.31	2019-10-22 14:23:51	Microsoft Windows 10 Pro 64비트
1	DESKTOP-C66KL2I	14.42.86.31	2019년 10월 22일 14시 23분 01초	Microsoft Windows 10 Home 64비트

처음 1 마지막

전체 개수: 7 개

개발 시스템 운영 (5/5)

현안 조치

- 앞 페이지의 진단 PC 목록에서 관심 PC를 지정하면 세부 진단사항을 웹 서비스로 제공하는 시스템을 개발 중

  ※ Vulmon의 스크립트 인터페이스 개발 등의 기술적 어려움으로 개발이 다소 지연

- 앞으로 1개월 이내 웹 서비스 시스템으로 진단정보를 획득 지원할 수 있는 시스템 개발을 완료할 예정

- 또한 취약점 횟수 누적에 따른 경고 시스템과 게시판을 통한 관리자와의 소통 및 안내사항 공지체제도 완성할 예정

결론 및 기대효과

❍ 결　　론

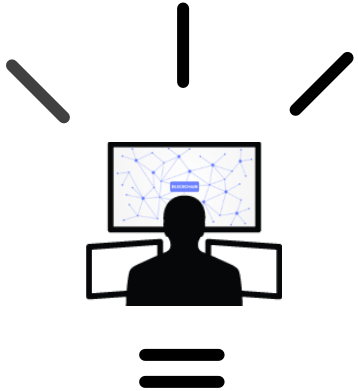
- 현재 개발중인 웹 서비스 체제를 구축하면 KISA 취약점 분석 평가 가이드에 기반한 OS 모니터링 시스템이 완성

- 다소 지연된 웹 서비스 체제 개발에 최선을 다하여 2019.11월 중 완성된 시스템을 구축할 예정

❍ 기대 효과

- OS 모니터링 시스템을 활용하여 관리자가 보안 취약점을 체계적으로 점검하고 적극적인 대응 처치가 가능할 것으로 기대

- 끝 -



Q&A

Thank you