



예방: 네트워크 탐색

Security Fundamentals

© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

보안 수명 주기: 예방 - 네트워크 탐색을 시작하겠습니다.

교육 내용

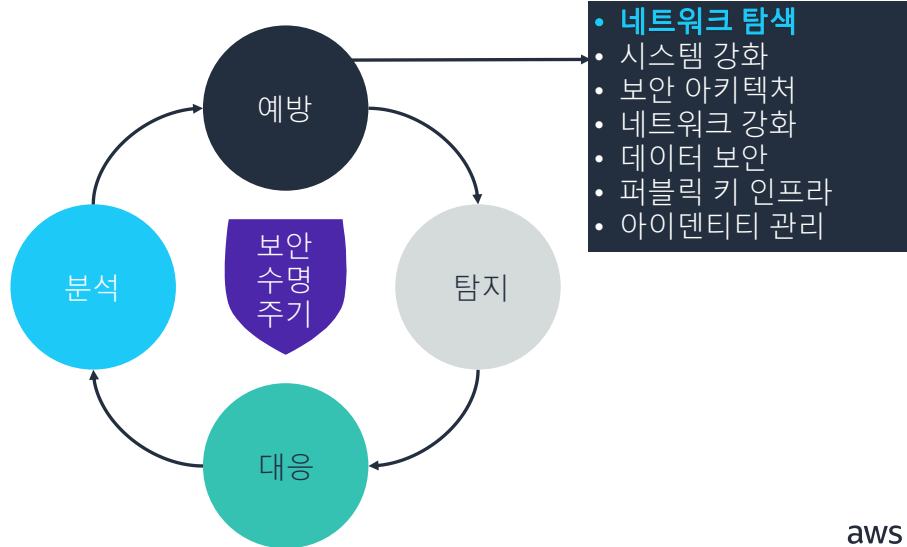
이 강의의 핵심

배울 내용은 다음과 같습니다.

- 초기의 전용 네트워크와 현대 네트워크에서 보안의 필요성을 비교합니다.
- 네트워크 환경을 보호하기 위한 계층화된 보안 모델의 이점을 설명합니다.
- 네트워크에 무엇이 있는지 발견하도록 해주는 다양한 도구를 파악합니다.



보안 수명 주기: 예방



3

aws re/start

복습하자면 보안 수명 주기는 이렇게 구성됩니다.

- **예방** - 첫 번째 방어선입니다.
- **탐지** - 예방이 실패했을 때 수행됩니다.
- **대응** - 보안 문제를 탐지했을 때 어떤 조치를 취할지 설명합니다.
- **분석** - 향후에 문제가 다시 발생하지 않도록 예방하는 새로운 예방 조치를 구현하면서 주기가 완료됩니다.

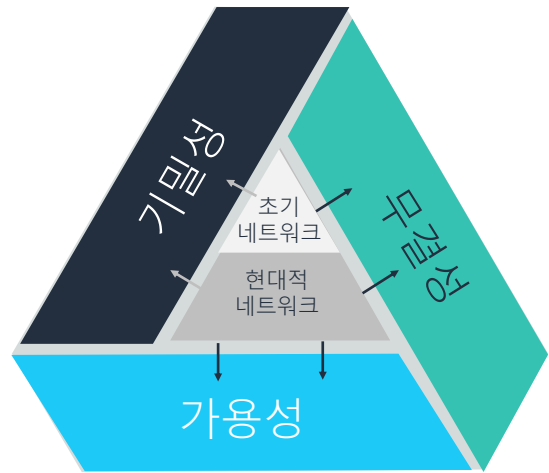
예방 단계에서 **네트워크 탐색**은 보안 제어를 구현하는 첫 번째 영역입니다. 네트워크 탐색은 여러분의 네트워크를 찾아 액세스할 수 있는 것을 말합니다.

네트워크 보안을 이해하려면 네트워크와 프로토콜을 이해하는 것이 중요합니다. 대상 네트워크에서 사용되는 **프로토콜**을 평가하는 과정에서 많은 취약성이 발견됩니다. 외부 주체는 **풋프린팅**, **스캐닝**, **열거법** 등의 기법을 사용하여 다음에 대한 기본적인 사실을 알아낼 수 있습니다.

- 내 온라인 상태
- 열려 있는 포트
- 내 시스템에 활성화된 서비스

네트워킹 검토

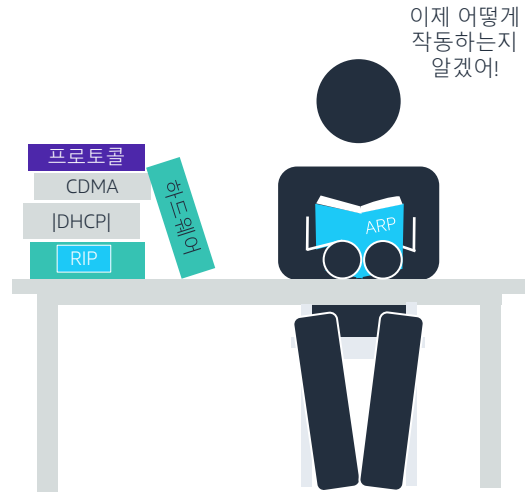
- 초기의 전용 네트워크는 기밀성과 무결성은 제공했지만 가용성은 제공하지 않았습니다.
- 현대적 네트워크:
 - 상호 연결성이 더 높음
 - 하루 24시간 액세스를 제공함
 - 몇 년 전보다 더 많은 대역폭을 사용함
- 가용성이 늘어나면서 기밀성과 무결성에 대한 요구도 높아집니다.



네트워크 취약성

취약성의 이유:

- 상대적으로 초기의 프로토콜은 전용 네트워크와 위험이 낮은 보안 이벤트만 고려함
- 암호화를 위한 추가 오버헤드는 정당화할 수 없음
- 어디에서나 액세스가 가능한 경우 위험이 증가함
- 공개 표준으로 인해 창의적인 부정 이용이 가능함



주소 결정 프로토콜(ARP)

네트워크 디바이스



라우터



방화벽



케이블 작업



NIDS



스위치



무선 AP



카메라



HIDS



프린터



센서



배지 또는
액세스 카드
프린터



IDS/IPS



스팸 또는
맬웨어 필터

6

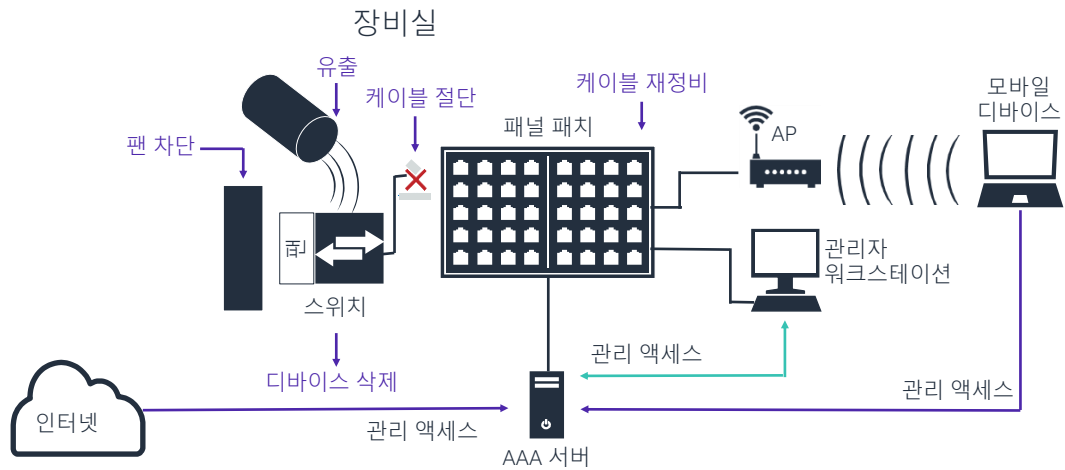
aws re/start

네트워크에는 다양한 유형의 디바이스가 포함될 수 있습니다. 각 디바이스를 평가하여 보안이 제대로 구현되었는지 평가하십시오. 또한 디바이스가 네트워크의 보안에 기여하는지 **여부, 어떻게** 기여하는지도 평가해야 합니다.

자주 사용되는 약어

- 침입 탐지 시스템(IDS)
- 네트워크 기반 침입 탐지 시스템(NIDS)
- 호스트 기반 침입 탐지 시스템(HIDS)
- 침입 방지 시스템(IPS)

침해된 액세스



네트워크 디바이스는 물리적 또는 관리적으로 침해될 수 있습니다.

네트워크의 디바이스를 보호하려면 디바이스가 물리적, 관리적으로 취약하다는 점을 고려하십시오.

AAA 서버: 인증, 권한 부여, 계정 관리(AAA) 서버

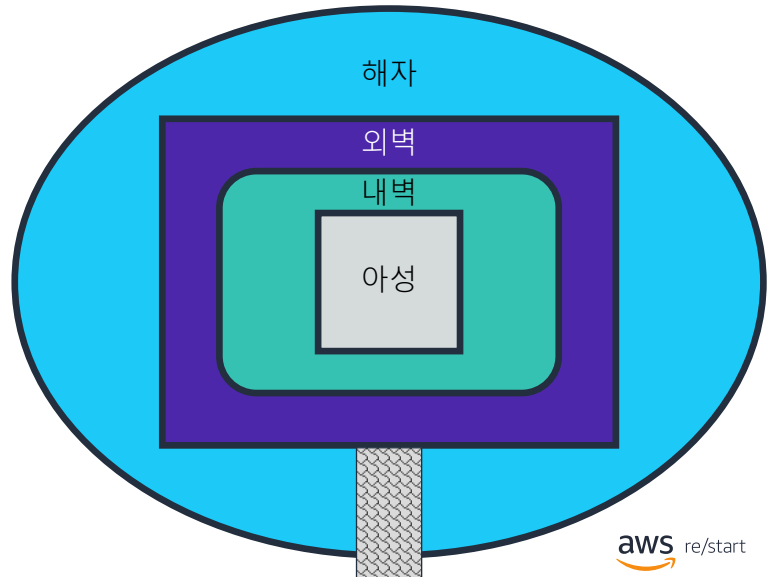


계층형 보안 모델

예: 계층형 방어



성



9

가장 좋은 보안 전략은 심층 방어로 접근하는 것입니다.

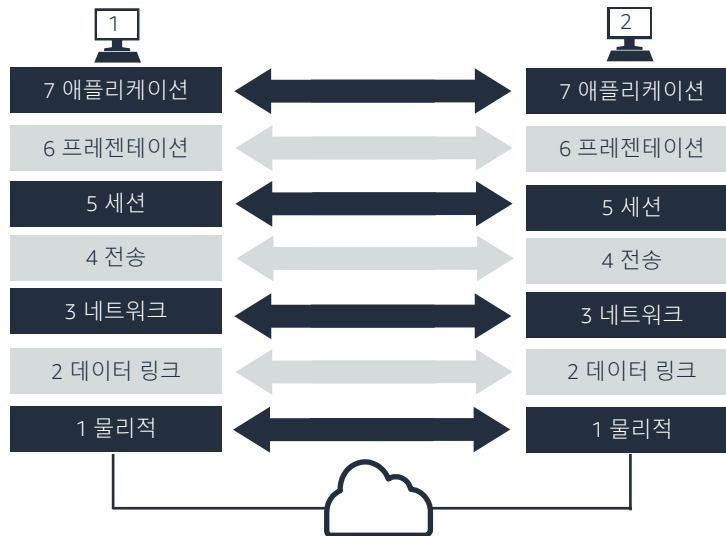
심층 방어란 외부 주체가 정보 또는 장비에 액세스하기 위해 침투해야 하는 여러 계층의 보안을 구현하는 것입니다.

예를 들어 성을 생각해 보십시오. 성에는 첫 번째 방어 수준으로 해자가 있을 수 있습니다. 그리고 외벽과 내벽, 그리고 아성이 있습니다. 공격군이 성을 점령하려면 각 계층을 격파해야 합니다.

마찬가지로, 기업에서는 시스템 침입을 더 어렵게 하기 위해 시스템에 많은 방어 계층을 구현합니다. 개방형 시스템 간 상호 접속(OSI) 모델의 각 계층에는 외부 주체가 그 계층을 침입하기 어렵게 만드는 방어 또는 보안 제어가 구현되어 있습니다. 계층마다 다양한 형태의 암호화가 사용되어 저장된 데이터와 네트워크 통신을 보호합니다. 방화벽과 IDS/IPS 디바이스는 각기 다른 계층의 침투를 탐지하고 예방하는 데 사용됩니다. 각 계층을 개별적으로 보호하여 외부 주체가 방어를 뚫고 리소스에 액세스하는 것을 최대한 어렵게 만드십시오.

예: OSI 모델

실제 OSI 모델



10

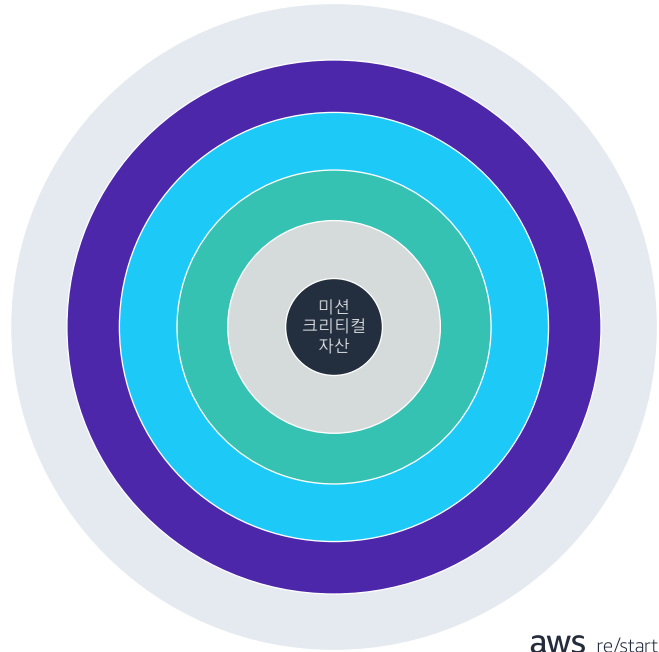
aws re/start

OSI 모델은 보안을 계층에 구현하는 또 다른 예를 제공합니다. 모델의 각 계층은 다음과 같은 보안 솔루션을 구현할 수 있는 기회가 됩니다.

- **물리적 계층** - 외부 침입자를 차단하기 위해 네트워크 디바이스와 장비가 물리적 액세스로부터 보호됩니다.
- **데이터 링크 계층** - 네트워크 스위치에 필터가 적용되어 매체 접근 제어(MAC) 주소를 기반으로 공격을 예방하는 데 도움이 됩니다.
- **네트워크 및 전송 계층** - 방화벽과 액세스 제어 목록(ACL)을 구현하면 내부 시스템에 무단 액세스를 줄이는 데 도움이 됩니다.
- **세션 및 프레젠테이션 계층** - 인증 및 암호화 방법을 사용하여 무단 데이터 액세스를 예방할 수 있습니다.
- **애플리케이션 계층** - 바이러스 스캐너, 침입 탐지 시스템(IDS)과 같은 솔루션으로 애플리케이션을 보호할 수 있습니다.

계층형 보안 모델

- 계층마다 자산에 서로 다른 수준의 방어를 제공합니다.
- 방어 수준:
 - 경계 보안
 - 네트워크 보안
 - 엔드포인트 보안
 - 애플리케이션 보안
 - 데이터 보안



11

aws re/start

보안 계층의 예:

- 경계 보안
 - 경계 방화벽
 - IDS 또는 IPS
 - 경계 네트워크(비무장 지대(DMZ)라고도 함)를 보호함
- 네트워크 보안
 - 네트워크 액세스 제어(NAC)
 - 기업 IDS 또는 IPS
 - 웹 프록시 콘텐츠 필터링
- 엔드포인트 보안
 - 데스크톱 방화벽
 - 호스트 IDP 또는 IPS
 - 콘텐츠 보안(바이러스 백신)
- 애플리케이션 보안
 - 동적 애플리케이션 테스트
 - 웹 애플리케이션 방화벽(WAF)
 - 데이터베이스 모니터링 및 스캐닝
- 데이터 보안
 - 아이덴티티 및 액세스 관리
 - 데이터 삭제 정리
 - 데이터 손실 방지(DLP)

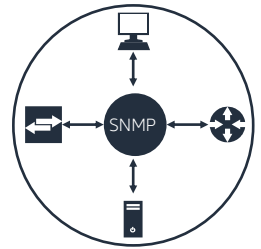


네트워크 탐색 도구

탐색, 풋프린팅, 스캐닝

- 네트워크 환경에 무엇이 있는지 찾아내는 도구입니다.
- 자동화된 네트워크 프로세스로 네트워크 정보를 가진 트래픽을 생성합니다.
- 기본 제어는 외부인이 네트워크에 들어오지 못하게 하는 것입니다.

감사 또는 포트 스캐닝



스니퍼

취약성 스캐너



aws re/start

13

외부 주체가 다음과 같이 다양한 도구와 기법을 사용하여 네트워크 환경을 찾을 수 있습니다.

- 풋프린팅 - 시스템에 침투하기 위해 시스템에 관해 최대한 많은 정보를 수집함
- 스캐닝 - 시스템 내의 보안 취약성을 검색하고 탐지함

이런 도구가 무엇인지 이해하고 이런 도구가 가져올 수 있는 보안 위험을 인식하는 것이 중요합니다.

탐색 도구



감사 또는 포트
스캐닝

- Nmap
- Zenmap
- SuperScan



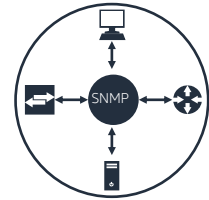
스니퍼

- OmniPeek
- Wireshark



ICMP:

- ping
- traceroute



SNMP:

- PowerSNMP
- SNMP Traffic Grapher
- Sensor SNMP CPU Load



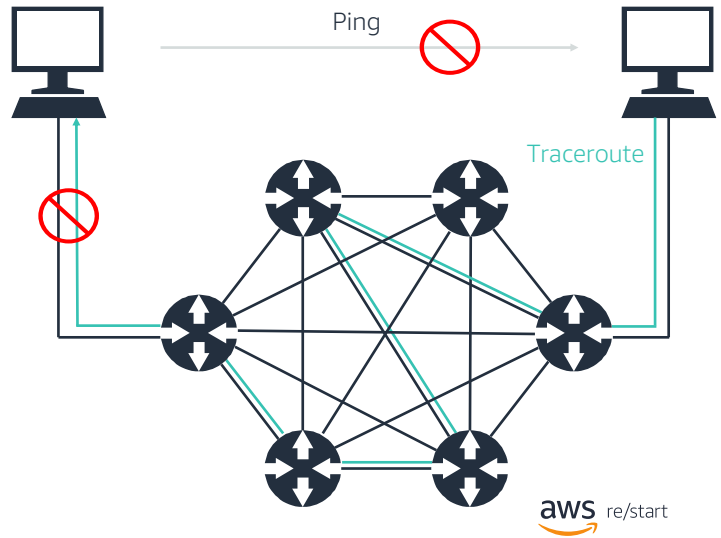
취약성 스캐너

- Nessus
- Retina

네트워크 환경에 관한 정보를 찾는 데 사용될 수 있는 일반적인 도구입니다.

인터넷 제어 메시지 프로토콜(ICMP)

- ICMP는 일반적으로 **ping** 및 **traceroute**와 관련이 있습니다.
- ICMP가 차단되면 사용자 컴퓨터에 도달하기 전에 ping과 traceroute의 전체 결과를 차단합니다.



가장 흔한 네트워크 탐색 도구에서는 인터넷 제어 메시지 프로토콜(ICMP)을 사용합니다. 예를 들어, **ping**과 **traceroute** 명령이 ICMP를 사용합니다.

분산 서비스 거부(DDoS) 공격과 같은 특정 유형의 공격으로부터 보호하기 위해 최소한 ICMP의 전체 사용을 제한하는 것이 좋습니다.

ICMP 예: Ping 및 Traceroute

이 간단한 명령을 사용하여 흥미로운 정보를 얻을 수 있습니다.

```
$ ping amazon.com
PING amazon.com (205.251.242.103): 56 data bytes
64 bytes from 205.251.242.103: icmp_seq=0 ttl=228 time=31.400 ms
64 bytes from 205.251.242.103: icmp_seq=1 ttl=228 time=32.249 ms
64 bytes from 205.251.242.103: icmp_seq=2 ttl=228 time=32.102 ms
64 bytes from 205.251.242.103: icmp_seq=3 ttl=228 time=32.415 ms
64 bytes from 205.251.242.103: icmp_seq=4 ttl=228 time=33.736 ms
^C
--- amazon.com ping statistics ---
6 packets transmitted, 5 packets received, 16.7% packet loss
round-trip min/avg/max/stddev = 31.400/32.380/33.736/0.761 ms
```

```
$ traceroute amazon.com
traceroute: Warning: amazon.com has multiple addresses; using 205.251.242.103
traceroute to amazon.com (205.251.242.103), 128 hops max, 62 byte packets
 1 * * *
 2 * * *
 3 * * *
 4 freeip.amazon.com (10.47.117.178) 34.050 ms 33.401 ms
   freeip.amazon.com (10.47.117.176) 38.240 ms
 5 * * *
 6 * * *
 7 * * *
 8 freeip.amazon.com (10.43.249.9) 33.295 ms 33.870 ms
   freeip.amazon.com (10.43.249.11) 31.198 ms
 9 iad7-7-np-edg-fw1.amazon.com (10.43.249.13) 29.670 ms 29.925 ms 29.768 ms
10 freeip.amazon.com (10.43.249.15) 30.883 ms 31.924 ms 31.101 ms
11 * * *
12 * * *
```

16

aws re/start


이 예에서는 amazon.com의 ping과 traceroute 출력을 보여줍니다.

Traceroute 명령의 출력을 통해 다음을 할 수 있습니다.

- 네트워크 디바이스의 이름을 살펴봄으로써 물리적 위치를 대략적으로 알아낼 수 있습니다. 예를 들면, iad7은 미국에 위치한 Amazon 데이터 센터입니다. IP 주소 또는 이름에 WHOIS(Who is)를 구현하면 추가 정보를 얻을 수 있습니다.
- 네트워크 경로와 응답 시간을 볼 수 있습니다.

추가 ping 또는 기타 ICMP 도구로 네트워크의 꽤 상세한 청사진을 만들 수 있습니다.

ICMP 예: IP 주소 소유자 식별



The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. [Learn more.](#)

Domain Names

IANA manages the DNS Root Zone (assignments of ccTLDs and gTLDs) along with other functions such as the .int and .arpa zones.

- Root Zone Management
- Database of Top Level Domains
- .int Registry
- .arpa Registry
- IDN Practices Repository

Number Resources

IANA coordinates allocations from the global IP and AS number spaces, such as those made to Regional Internet Registries.

- IP Addresses & AS Numbers
- Network abuse information

Protocol Assignments

IANA is the central repository for protocol name and number registries used in many Internet protocols.

- Protocol Registries
- Apply for an assignment
- Time Zone Database

Responsible organisation: Global Telephone & Telecommunication S.A. (GT&T)
Abuse contact info: abuse@globaltt.com

inetnum: 217.30.16.0 - 217.30.16.255
netname: GTT-NETWORK
descr: PROVIDER Local Registry
descr: Global Telephone & Telecommunication S.A.
country: BE
admin-c: JG1268-RIPE
tech-c: GG2670-RIPE
status: ASSIGNED PA
notify: ripe-admin@globaltt.com
mnt-by: GLOBALTT-PWIT
mnt-lower: GLOBALTT-PWIT
mnt-routes: GLOBALTT-PWIT
created: 2004-02-11T16:58:58Z
last-modified: 2004-10-06T08:23:42Z
source: RIPE

For details for 217.30.16

Network	
Net Range	68 142 192 0 - 68 142 255 255
CIDR	68 142 192 0/8
Name	NET68-BLK-4
Handle	NET68-142-192-0-1
Parent	NET68 (NET-68-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Infotim Corporation (INF)
Registration Date	2004-03-24
Last Updated	2012-02-24
Comments	
RESTful Link	https://ripe.net/whois/ripe/NET-68-142-192-0-1

Function Information

Function	Point of Contact
Abuse	NET68@INF (NET68@INF, ARIN)

See Also

Related organization's POC records

See Also

Related delegations

Internet Assigned Numbers Authority(IANA) 웹 사이트를 사용하여 공인 IP 주소의 소유자에 관한 정보를 찾을 수 있습니다. 다음 단계를 따르면 됩니다.

1. 브라우저에서 iana.org로 이동합니다.
IANA는 전 세계의 IP 주소를 할당하는 조직입니다.
2. **Number Resources** 섹션에서 **IP Addresses & AS Numbers** 링크를 선택합니다.
이 페이지에서는 다섯 개의 Regional Internet Registries(RIR)로 연결되는 링크를 제공합니다. 각 RIR은 전 세계에서 특정 리전의 IP 주소를 관리할 책임이 있습니다.
3. 링크를 선택하여 **American Region of Internet Numbers(ARIN)** 사이트를 방문합니다.
ARIN은 북미의 번호를 관리하는 책임을 집니다. 여러분이 북미에서 작업하는 경우 조사하는 IP 주소가 북미에 있을 가능성이 큼니다. 여러분이 북미에 있지 않은 경우 ping하는 조직이 미국이나 캐나다에 있다면 ARIN 사이트를 사용해서 검색을 시작하십시오.
4. ARIN 사이트의 오른쪽 상단에 있는 검색란에 조사할 IP 주소를 입력하고 **Search**를 선택합니다.
검색 결과가 표시됩니다. 여러분의 IP 주소가 여러 IP 주소의 네트워크 블록에 속한 것으로 나옵니다. 조직의 경우, 특히 대규모 조직의 경우 블록이 나오는 경우가 많습니다.

IP 주소의 소유자에 관한 정보는 페이지의 하단 섹션에 포함되어 있습니다.

Nmap

Nmap은 ICMP 및 기타 프로토콜을 사용하여 네트워크 데이터를 수집 및 제시하는 네트워크 매핑 도구입니다.

```
C:\nmap-3.81>nmap.exe -O 192.168.1.107 -p 25,80,135,137,139,445

Nmap for Windows v3.81
Original version (WinPCap is required) : http://www.insecure.org/nmap
This version (works without WinPCap)  : http://packetstuff.com
Compiled with Packet Sniffer SDK v2.3  : http://microolap.com/pssdk

Starting nmap 3.81 < http://www.insecure.org/nmap > at 2006-05-20 13:23 Eastern
Daylight Time
Interesting ports on U2KLAB (192.168.1.107):
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
135/tcp    open  msrpc
137/tcp    closed nethios-ns
139/tcp    open  nethios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:B0:16:54 (VMware)
Device type: general purpose
Running: Microsoft Windows 95/98/ME/NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Pro or Advanced Server, or Windows XP, Microsoft Windows 2000 SP3

Nmap finished: 1 IP address (1 host up) scanned in 4.500 seconds

C:\nmap-3.81>
```

aws re/start

18

네트워크에 관한 정보를 수집하는 데 사용할 수 있는 다른 도구는 다음과 같습니다.

- Nmap - Linux, Microsoft Windows, macOS에서 사용할 수 있는 네트워크 매핑
- Zenmap - Nmap의 GUI 기반 버전
- SuperScan - Microsoft Windows 사용자용 도구

프로토콜 분석기

- 프리웨어, 셰어웨어, 상업용 등 다양한 버전을 제공합니다.
- 대부분 수동적 도구입니다.
- 교환된 네트워크와 암호화를 사용하여 네트워크에서 유용성을 제어합니다.
- 대부분의 사용자가 네트워크에서 이런 도구를 실행하는 것을 정책으로 금지합니다.



Omnipeek

The screenshot shows the Wireshark interface with a list of captured packets. The columns include No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered by 'eth II > 0' and show various protocols like TCP, UDP, and HTTP.

Wireshark

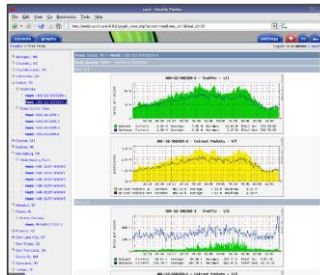
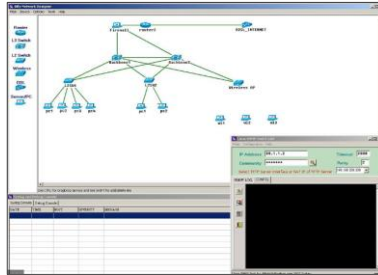
aws re/start

스니퍼라고도 하는 프로토콜 분석기는 네트워크를 통과하는 모든 트래픽을 수동적으로 감시하고 저장합니다. 그런 다음 수집한 정보를 사람이 읽을 수 있는 형식으로 변경합니다. 암호화되지 않은 모든 트래픽은 읽을 수 있는 형식으로 재구성될 수 있습니다. 추후에 저장된 패킷 캡처를 검토하고 다른 사람과 공유할 수 있습니다.

슬라이드의 화면 캡처에는 Omnicap과 Wireshark 프로토콜 분석기가 나와 있습니다.

간이 망 관리 프로토콜(SNMP)

- SNMP 도구는 대개 네트워크 운영 센터(NOC) 또는 헬프 데스크에서 사용됩니다.
- 강화되지 않은 경우 외부 주체가 SNMP를 사용하여 환경에 대해 많은 세부 정보를 발견할 수 있습니다.



간이 망 관리 프로토콜(SNMP)은 네트워크 트래픽을 탐색하는 데 사용될 수 있는 또 다른 메커니즘입니다. 따라서 SNMP의 가용성을 신중하게 평가하여 보안 공격을 보호하기 위해 사용해야 합니다.

Common Vulnerabilities and Exposures

- 공개적으로 알려진 정보 보안 취약성 및 노출을 나열합니다.
- 다양한 취약 데이터베이스와 보안 도구의 데이터를 공유합니다.
- MITRE Corporation에서 유지 관리하며 NCSD에서 후원합니다.

CVE(버전 20061101) 및 20161006 기준 후보

후보가 공식 CVE 목록에 추가되려면 CVE 편집국의 검토와 수락을 거쳐야 합니다. 따라서 이 후보는 향후에 수정 또는 거부될 수 있습니다. 후보 목록은 편집국에서 완전히 검토를 거치지 않은 항목에 대해 조기에 번호 지정 체계가 필요한 개인을 위해 제공됩니다.

이름: CVE-1999-0001

설명:

ip_input.c in BSD-derived TCP/IP를 구현하면 원격 공격자가 만들어진 패킷을 통해 서비스 거부(충돌 또는 종료)를 일으킬 수 있습니다.

상태: 후보

단계: 수정됨(20051217)

참조: CERT:CA-98-13-tcp-denial-of-service

참조: BUGTRAQ:19981223 Re: CERT Advisory CA-98.13 - TCP/IP Denial of Service

참조: CONFIRM:<http://www.openbsd.org/errata23.html#tcpfix>

참조: OSVDB:5707

참조: URL:<http://www.osvdb.org/5707>

[Common Vulnerabilities and Exposures\(CVE\) 웹 사이트](#)는 공개적으로 노출된 사이버 보안 취약성을 나열한 온라인 리소스입니다. MITRE Corporation에서 유지 관리하고 National Cyber Security Division(NCSD)에서 후원합니다. 일부 스캐닝 도구는 특정 CVE를 노릴 수 있습니다.

추가 리소스

- 사이버 위협 지도
 - 현재 사이버 위협 전장이 어떤 모습인지 궁금한 적이 있으셨습니까? 많은 사이트에서 전 세계에서 벌어지고 있는 사이버 공격을 실시간으로 보여줍니다.
 - 그 중 하나가 [Cyberthreat Real-time Map](#)입니다.

보안 정책

- 고위 경영진에서 위험 관리 의사결정을 기반으로 정책을 정의합니다.
- 관리적 제어로 물리적 및 기술적 제어에 대한 의사결정을 내립니다.
- 네트워크 보안 정책은 다음 사항을 다룹니다.
 - 액세스할 수 있는 사람
 - 각 사람에게 주어진 사용량
 - 각 직원이 갈 수 있는 위치
 - 연결될 수 있는 항목 또는 연결될 수 없는 항목



정책을 관리적 제어로 사용하여 조직에 보안 조치를 시행하십시오. 조직의 건전한 상태와 존립을 위해 올바른 보안 정책을 구현하는 것이 필수입니다.

핵심 사항



© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

23

- 계층형 보안 모델은 네트워크의 리소스를 보호하는 효과적인 방법입니다.
- 프로토콜을 부정 이용하는 공격으로부터 보호하기 위해 ICMP, SNMP 등 프로토콜의 전체 사용을 제한하는 방법을 고려해 보십시오.
- 조직에서 자산을 보호하기 위해 보안 정책을 구현해야 합니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- 계층형 보안 모델은 네트워크의 리소스를 보호하는 효과적인 방법입니다.
- 프로토콜을 부정 이용하는 특정 유형의 공격으로부터 보호하기 위해 ICMP, SNMP 등 프로토콜의 전체 사용을 제한하는 방법을 고려해 보십시오.
- 조직에서 자산을 보호하기 위해 보안 정책을 구현해야 합니다.