



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2016년02월15일

(11) 등록번호 10-1593897

(24) 등록일자 2016년02월04일

(51) 국제특허분류(Int. Cl.)

H04L 12/22 (2006.01) H04L 12/26 (2006.01)

(21) 출원번호 10-2014-0178034

(22) 출원일자 2014년12월11일

심사청구일자 2014년12월11일

(56) 선행기술조사문헌

<http://web.archive.org/web/20130822162202/http://www.hainsoft.com/howto-scan-network.htm>*

KR1020050036457 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

이상진

서울특별시 종로구 사직로8길 20, 101동 1503호 (내수동, 파크팰리스)

김도수

서울특별시 동대문구 무학로49길 14, 302호 (용두동)

(뒷면에 계속)

(74) 대리인

특허법인충현

전체 청구항 수 : 총 5 항

심사관 : 윤태섭

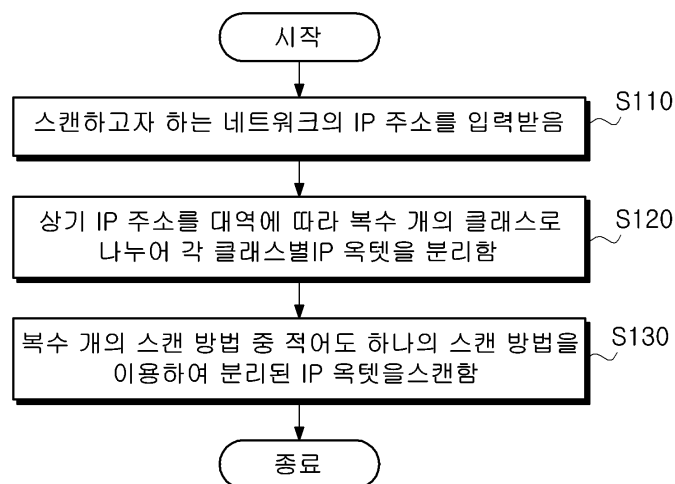
(54) 발명의 명칭 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법

(57) 요약

본 발명은 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법에 관한 것으로서, 보다 바람직하게는 입력부가 스캔하고자 하는 네트워크의 IP 주소를 입력받는 단계; IP옥텟분리부가 상기 IP 주소를 대역에 따라 복수 개의 클래스로 나누어 각 클래스별 IP 옥텟(Octet)을 분리하는 단계; 및 네트워크 스캐너가 복수 개의 스캔 방법 중 적어도 하나의 스캔 방법을 이용하여 분리된 IP 옥텟을 스캔하는 단계;를 포함한다.

이러한 구성에 의해, 본 발명의 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법은 네트워크 상황에 따라 적합한 스캔방법을 선택하여 IP 옥텟 중 A 옥텟부터 D 옥텟까지 순차적으로 옥텟을 변화하며 스캔함으로써, 내부 네트워크에 별도의 설정없이도 방화벽을 우회하면서도 용이하게 네트워크를 스캔할 수 있는 효과가 있다.

대표도 - 도1



(72) 발명자

김정현

인천광역시 중구 서해대로464번길 6, 202호 (신흥동2가, 미성홈타운)

안휘항

서울특별시 관악구 봉천로23다길 59-7 (봉천동)

최중현

서울특별시 동대문구 천장산로6길 35-4 (이문동)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711014052

부처명 미래창조과학부

연구관리전문기관 정보통신산업진흥원

연구사업명 정보통신기술인력양성

연구과제명 제어시스템 보안 연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2014.01.01 ~ 2014.12.31

특허청구의 범위

청구항 1

입력부가 스캔하고자 하는 네트워크의 IP 주소를 입력받는 단계;

IP옥텟분리부가 상기 IP 주소를 대역에 따라 A, B, C, D를 포함하는 복수 개의 클래스로 나누어 각 클래스별 IP 옥텟(Octet)을 분리하는 단계; 및

네트워크 스캐너가 복수 개의 스캔 방법 중 적어도 하나의 스캔 방법을 이용하여 분리된 IP 옥텟을 A 옥텟부터 D 옥텟까지 순차적으로 증가시키며 스캔함으로써, 방화벽, IDS 또는 IPS로 하여금 정상적인 접근으로 판단하도록 유도하는 단계;

를 포함하는 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법.

청구항 2

제1항에 있어서,

상기 방화벽, IDS 또는 IPS로 하여금 정상적인 접근으로 판단하도록 유도하는 단계는

상기 네트워크의 상황에 따라 ICMP Sweep scan 방법, TCP Connect scan 방법, Half-open scan 방법, TCP Ack scan 방법, Stealth scan 방법 중 적어도 하나의 스캔방법을 이용하여 상기 IP 옥텟을 스캔하는 것을 특징으로 하는 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법.

청구항 3

제1항에 있어서,

상기 방화벽, IDS 또는 IPS로 하여금 정상적인 접근으로 판단하도록 유도하는 단계는

분리된 IP 옥텟이 1부터 255까지 사용하는 것을 특징으로 하는 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법.

청구항 4

제1항에 있어서,

방화벽, IDS 또는 IPS로 하여금 정상적인 접근으로 판단하도록 유도하는 단계는

분리된 IP 옥텟을 통해 복수 개의 IP 그룹이 생성된 경우, 상기 복수 개의 IP 그룹에 대하여 분산 처리를 수행하는 것을 특징으로 하는 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법.

청구항 5

제1항 내지 제4항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명세서

기술분야

본 발명은 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법에 관한 것으로, 특히 방화벽, IDS 또는 IPS가 설치된 네트워크에 대해서도 별도의 설정없이 용이하게 방화벽, IDS 또는 IPS를 우회하며 해킹으로 오인되지 않

[0001]

고, 정상적으로 네트워크를 스캔할 수 있는 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법에 관한 것이다.

배경 기술

- [0002] 최근 들어, IT 기술의 급격한 발전으로 인하여 남녀노소를 막론하고, PC, 스마트폰, 태블릿 PC 등과 같은 다양한 형태의 전자기기를 사용하고 있으며, 이러한 전자기기들은 상호간에 네트워크를 형성한다.
- [0003] 이러한 전자기기들은 네트워크를 통해 유포되는 각종 형태의 바이러스 등에 노출되는 것을 미연에 방지하기 위해, 내부적으로 방화벽, IDS 또는 IPS를 이용하고 있다.
- [0004] 이때, 사용되는 방화벽은 인터넷 프로토콜(IP)로 접속되어 있는 네트워크를 불법적인 침입으로부터 보호하기 위하여 게이트웨이에 설치되는 접속 제한을 나타낸다.
- [0005] 특히, 인터넷에서는 한쪽 방향의 접속이 가능하면 역방향의 접속도 가능하기 때문에 IP로 접속되어 있는 네트워크는 외부에서도 접속이 가능하다. 이에 따라, 상기 방화벽을 통해 외부 단말에 대한 네트워크의 접속을 제한함으로써 어느 정도의 보안을 확보할 수 있는데, 구체적으로는 네트워크 간의 IP 패킷 전송을 차단하는 방법, 특정의 애플리케이션에 의한 패킷만을 전송하도록 하는 방법 등이 있다.
- [0006] 뿐만 아니라, IDS(Intrusion Detection System)는 침입 탐지 시스템을 나타내는 것으로서, 정보시스템의 보안을 위협하는 침입행위가 발생할 경우를 탐지하고, 적극 대응하기 위한 시스템을 나타낸다. 특히, 상기 침입 탐지 시스템은 네트워크 내 침입차단을 목적으로 하는 방화벽과는 달리, 각종 해킹 수법을 이미 내부 메모리에 내장하고 있어 침입행동을 실시간으로 감지하거나, 제어 또는 추적할 수 있다.
- [0007] 만약, 해킹 사실이 발견됐을 때는, 해킹에 관한 정보를 이동전화, 전자우편 등으로 즉시 전송하고, 네트워크 관리자가 없을 경우에도 24시간 시스템 보안을 유지한다. 따라서, 내부 정보의 유출도 사전에 탐지하여 미리 차단하고, 침입을 시도한 해커에 대해서는 침투경로까지 추적하여 찾아내며, 데이터를 안전한 곳으로 전환시켜 놓는 등과 같이, 방화벽의 수동적인 대처와는 달리 적극적인 대응을 한다.
- [0008] 또한, IPS(Intrusion Prevention System)는 침입 방지 시스템으로서, 외부 네트워크로부터 내부 네트워크로 침입하는 네트워크 패킷을 찾아 제어하는 기능을 가진 소프트웨어 또는 하드웨어를 나타낸다. 일반적으로는 내부 네트워크로 들어오는 모든 패킷이 지나가는 경로에 상기 IPS가 설치되며, 호스트의 IP주소, TCP/UDP의 포트번호, 사용자 인증에 기반을 두고 외부 침입을 차단하는 역할을 하며, 허용되지 않는 사용자나 서비스에 대해 사용을 거부하여 내부 자원을 보호한다.
- [0009] 이와 같이, 상술한 방화벽, IDS 또는 IPS가 네트워크 스캐닝을 탐지하여 특정 IP를 갖는 단말의 네트워크 접속을 차단함으로써, 해커들의 각종 공격을 방지하고 있다.
- [0010] 하지만 이러한 방화벽, IDS, IPS를 이용해 해커들의 공격을 방지하는 경우에, 해커의 공격이 아니며, 정상적인 네트워크 스캔임에도 불구하고, 해커의 공격으로 오인되어 정상적인 네트워크 스캔이 수행되지 못하는 문제점이 발생했다.

선행기술문헌

특허문헌

- [0011] (특허문헌 0001) KR 10-0584587 (네트워크 스캐너 및 네트워크 스캔 시스템 구성 및 유지방법, 삼성전자주식회사) 2006.05.23.

발명의 내용

해결하려는 과제

- [0012] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 스캔하고자 하는 네트워크 상황에 따라 적합한 스

캔방법을 선택하여 IP 옥텟 중 A 옥텟부터 D 옥텟까지 순차적으로 스캔함으로써, 내부 네트워크에 별도의 설정 없이도 기설치된 방화벽을 우회하여 용이하게 네트워크를 스캔하는 방법을 제공하고자 한다.

과제의 해결 수단

- [0013] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법은 입력부가 스캔하고자 하는 네트워크의 IP 주소를 입력받는 단계; IP옥텟분리부가 상기 IP 주소를 대역에 따라 복수 개의 클래스로 나누어 각 클래스별 IP 옥텟(Octet)을 분리하는 단계; 및 네트워크 스캐너가 복수 개의 스캔 방법 중 적어도 하나의 스캔 방법을 이용하여 분리된 IP 옥텟을 스캔하는 단계;를 포함한다.
- [0014] 보다 바람직하게는 상기 네트워크의 상황에 따라 ICMP Sweep scan 방법, TCP Connect scan 방법, Half-open scan 방법, TCP Ack scan 방법, Stealth scan 방법 중 적어도 하나의 스캔방법을 이용하여 상기 IP 옥텟을 스캔하는 네트워크 스캐너가 적어도 하나의 스캔 방법을 이용하여 IP 옥텟을 스캔하는 단계를 포함할 수 있다.
- [0015] 특히, 분리된 IP 옥텟 중 A 옥텟부터 D 옥텟까지 순차적으로 스캔하는 네트워크 스캐너가 적어도 하나의 스캔 방법을 이용하여 IP 옥텟을 스캔하는 단계를 포함할 수 있다.
- [0016] 보다 바람직하게는 분리된 IP 옥텟을 통해 복수 개의 IP 그룹이 생성된 경우, 상기 복수 개의 IP 그룹에 대하여 분산 처리를 수행하는 네트워크 스캐너가 적어도 하나의 스캔 방법을 이용하여 IP 옥텟을 스캔하는 단계를 포함할 수 있다.

발명의 효과

- [0017] 본 발명의 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법은 네트워크 상황에 따라 적합한 스캔방법을 선택하여 IP 옥텟 중 A 옥텟부터 D 옥텟까지 순차적으로 옥텟을 변화하며 스캔함으로써, 내부 네트워크에 별도의 설정없이도 방화벽을 우회하면서도 용이하게 네트워크를 스캔할 수 있는 효과가 있다.

도면의 간단한 설명

- [0018] 도 1은 본 발명의 일 실시 예에 따른 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법을 나타낸 순서도이다.
- 도 2는 본 발명에서 사용되는 복수 개의 스캔 방법을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0019] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.
- [0020] 이하, 도 1을 참조하여, 본 발명의 일 실시 예에 따른 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔방법에 대하여 자세히 살펴보도록 한다.
- [0021] 도 1은 본 발명의 일 실시 예에 따른 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법을 나타낸 순서도이다.
- [0022] 도 1에 도시된 바와 같이, 본 발명의 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법은 각종 입출력 장치, 마이크로 프로세서 및 메모리를 통해 구현되는데, 먼저 입력부가 스캔하고자 하는 네트워크 내 대상 시스템에 대한 IP 주소를 입력받는다(S110). 이때, 상기 IP 주소(Internet Protocol Address)란 컴퓨터끼리 서로 통신을 하기 위한 고유번호로서, 32비트(4바이트)의 길이를 가진다.
- [0023] 이후, IP옥텟분리부가 상기 IP 주소를 대역에 따라 복수 개의 클래스로 나누어 각 클래스별 IP 옥텟(Octet)을 분리한다(S120). 이러한 IP옥텟분리부는 네트워크를 나누는 기준으로 클래스(Class)라는 개념을 사용하여 IP 대역대를 기준으로 A, B, C, D, E 클래스로 분류하고 있으며, 이때 8비트(1바이트)를 옥텟이라 한다.

표 1

[0024]

클래스	첫째 옥텟 값 범위	IP 주소 범위
A 클래스	0~127	0.0.0.0 ~ 127.255.255.255
B 클래스	128~191	128.0.0.0 ~ 191.255.255.255
C 클래스	192~223	192.0.0.0 ~ 233.255.255.255
D 클래스	224~239	224.0.0.0 ~ 239.255.255.255
E 클래스	240~255	240.0.0.0 ~ 255.255.255.255

[0025]

상기 표 1에 기재된 바와 같이, 클래스 A는 대규모 네트워크 환경에 쓰이며, IP 주소 4마디 중 첫 번째 마디의 숫자가 0 내지 127(약 1,600만 개 IP 주소 사용 가능)까지 사용된다. 클래스 B는 중규모 네트워크 환경용으로 128 내지 191(약 65,000개 IP 주소 사용 가능)까지, 클래스 C는 소규모 네트워크 환경에 적용되는 것으로 192 내지 223(254개 IP 주소 사용 가능)까지 사용된다. 또한 클래스 D와 E가 223 이후의 숫자로 구성되는데, 이는 연구개발용 IP 주소이므로 일반적인 용도로 활용되지 않는다.

[0026]

이와 같이, 클래스가 분류된 IP 주소는 8 비트씩 4개로 끊어 표기하는데, 이때 각 마디에 해당하는 8 비트를 IP 옥텟으로 표기한다.

[0027]

이에 따라, 상기 IP 옥텟은 A 옥텟부터 D 옥텟까지로 이루어지며, 일반적인 IP는 D 옥텟을 기반으로 호스트에게 할당한다.

[0028]

이어서, 네트워크 스캐너가 복수 개의 스캔 방법 중 적어도 하나의 스캔 방법을 이용하여 분리된 IP 옥텟을 스캔한다(S130).

[0029]

특히, 종래의 D 옥텟부터 스캔하는 방법은 같은 기관 또는 회사의 네트워크를 단기간 동안 여러 번에 걸쳐 접근하게 되는데, 이처럼 하나의 기관 또는 회사의 네트워크를 여러 포트로 단기간 동안 접근하는 경우, 방화벽 및 IDS/IPS에서 차단할 가능성이 높다. 따라서, 상기 네트워크 스캐너가 IP 주소의 A 옥텟부터 D 옥텟까지 순차적으로 증가시키며 스캔하여 타겟 시스템이 비정상적인 접근으로 판단하여 차단하지 않도록 스캔한다.

[0030]

이러한 네트워크 스캐너는 네트워크 상황에 따라 복수 개의 스캔 방법 중 적어도 하나의 스캔 방법을 이용하여 IP 옥텟을 스캔하는데, 이때 사용되는 복수 개의 스캔 방법은 ICMP Sweep scan 방법, TCP Connect scan 방법, Half-open scan 방법, TCP Ack scan 방법, Stealth scan 방법 중 적어도 하나가 될 수 있다.

[0031]

이하에는 상기 복수 개의 스캔 방법에 대하여 도 2를 참조하여 자세히 살펴보도록 한다.

[0032]

첫째, ICMP Sweep 스캔 방법은 대상 네트워크 또는 시스템에 ICMP echo_request 패킷을 순차적으로 전송한 후, 상기 echo_request 패킷에 대한 응답 메시지인 echo_reply를 기반으로 해당 시스템의 동작 여부를 결정하는데, 이러한 과정을 ping sweep이라고 한다. 이러한 ping sweep은 소규모 네트워크 환경에서 신속하게 시스템의 동작 여부를 점검할 수 있는 장점이 있다. 하지만 상대적으로 규모가 큰 네트워크 환경에서는 많은 시간이 소요되어 비효율적일 뿐만 아니라, 보안상 ICMP를 막아두는 네트워크 환경에서는 상기 ICMP sweep 스캔 방법을 이용할 수 없다는 단점이 있다.

[0033]

도 2는 본 발명에서 사용되는 복수 개의 스캔 방법을 나타낸 도면이다.

[0034]

도 2(a)에 도시된 바와 같이, 두 번째, TCP Connect 스캔 방법은 TCP 프로토콜의 3-way 핸드셰이킹(handshaking)을 이용해 각 포트에 접속을 시도해 완전한 TCP 연결을 맺기 때문에 신뢰성 있는 결과를 얻을 수 있다. 하지만 이러한 TCP Connect 스캔 방법은 속도가 느리고 로그가 남기 때문에 쉽게 탐지될 수 있다는 단점이 있다. 이러한 TCP Connect 스캔 방법은 스캔하고자 하는 대상 시스템의 해당 포트가 개방되어 있는 경우에는, 네트워크 스캐너가 해당 IP 주소를 갖는 대상 시스템으로 SYN/ACK 패킷을 전송하며, 포트가 닫혀있는 경우에는 RST/ACK 패킷을 전송한다.

[0035]

세 번째, Half-open 스캔 방법은 도 2(b)에 도시된 바와 같이, TCP Syn 스캔 방법이라고 하며, TCP SYN 패킷을

이용해 대상 시스템으로의 접속을 시도하고, 포트가 열려있는 경우에는 응답 패킷인 SYN/ACK에 대해 접속을 강제 종료(RST)하여 정상적인 TCP 3-way 핸드셰이킹 과정을 맺지않는 스캔 방법이다. 이러한 스캔 방법의 경우, 대상 시스템의 해당 포트가 개방되면, 본 발명의 네트워크 스캐너가 SYN/ACK 패킷을 전송하고, 상기 대상 시스템의 해당 포트가 닫혀있는 경우에는 RST/ACK 패킷을 전송한다.

[0036] 네 번째, TCP Ack 스캔 방법은 도 2(c)에 도시된 바와 같이, 네트워크 스캐너가 초기의 SYN 패킷 대신 ACK 패킷을 대상 시스템으로 전송하는데, 이는 다수의 패킷 필터링 장비가 네트워크에서 연결이 성립된 세션은 허용한다는 것을 이용하며, IPS와 같은 보안 장비의 패킷 필터링 기능을 우회하여 내부 네트워크를 스캔한다. 이에 따라, 대상 시스템의 해당 포트가 개방되어 있는 경우에, 네트워크 스캐너가 상기 대상 시스템으로 RST 패킷을 전송하며, 포트가 닫혀있는 경우에는 RST/ACK 패킷을 전송하게 된다.

[0037] 마지막으로, Stealth 스캔 방법은 도 2(d)에 도시된 바와 같이, 공통적으로 TCP 헤더의 각 플래그 값을 인위적으로 조작하는 방법을 나타내는 것으로, 대다수 시스템에서는 이런 접속에 대해 로그를 남기지 않으므로 발견될 확률이 매우 낮은 스캔 방법이다. FIN 스캔은 FIN 플래그를, XMAS 스캔은 모든 플래그를 활성화하며, NULL 스캔은 이와 반대로 모든 플래그를 비활성화한 값을 사용한다. 이러한 세 가지 스캔 방법은 공통적으로 대상 포트가 열려있으면 아무런 응답이 없고, 대상 포트가 닫혀 있으면 해당 호스트는 공격자에게 RST 패킷을 전송한다.

[0038] 이에 더하여, 분리된 IP 옥텟을 통해 복수 개의 IP 그룹이 생성된 경우, 효율적인 처리를 위해, 상기 복수 개의 IP 그룹에 대하여 분산 처리를 수행할 수 있다. 이러한 분산처리 과정을 통해, 일정 기간 동안 주기적으로 네트워크 스캐닝을 하는 것을 탐지하는 방화벽이나 IDS/IPS를 우회할 수 있다. 또한 분산처리를 하는 동안 방화벽이나, IDS/IPS에서 탐지하지 못하도록 일정 시간동안 대기할 수도 있다.

[0039] 이러한 상기 네트워크 스캐너의 상태를 유휴(IDLE), 사용중(BUSY), 로그인 또는 에러를 통해, 현재 네트워크의 스캔 상태를 사용자에게 알려줄 수 있다. 이때, 상기 유휴 상태는 네트워크 스캐너가 현재 사용가능한 상태를 나타내는 값이고, 상기 사용 중인 상태는 네트워크 스캐너가 현재 스캔을 수행중인 상태를 나타내는 값이다. 상기 로그인은 사용자가 로그인한 상태를 나타내는 값이고, 에러는 네트워크 스캐너에 문제가 생겼음을 나타내는 값이다.

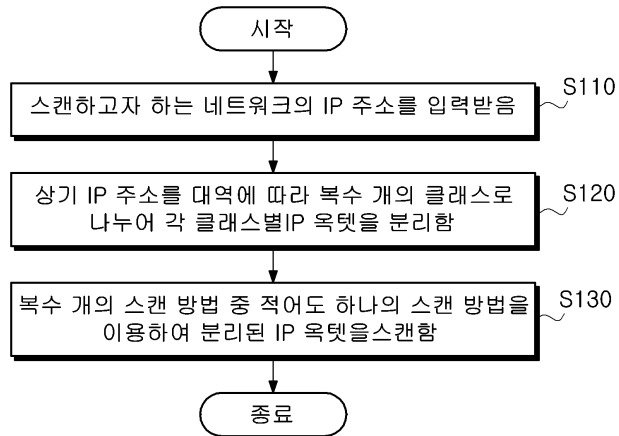
[0040] 또한, 이러한 본 발명의 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법은 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체에 저장될 수 있다. 이때, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0041] 본 발명의 방화벽, IDS 또는 IPS를 우회하는 네트워크 스캔 방법은 네트워크 상황에 따라 적합한 스캔방법을 선택하여 IP 옥텟 중 A 옥텟부터 D 옥텟까지 순차적으로 옥텟을 변화하며 스캔함으로써, 내부 네트워크에 별도의 설정없이도 방화벽을 우회하면서도 용이하게 네트워크를 스캔할 수 있는 효과가 있다.

[0042] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

도면

도면1



도면2

