creative commons

COMMONS DEED

저작자표시-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이 저작물을 영리 목적으로 이용할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

공학석사학위논문

실제 대용량 공격 로그의 직접적 분석으로 밝힌 공격형태

Features of attacks based on the direct analysis of real bulk attack logs

2015년 2월

서울대학교 대학원
전기・컴퓨터 공학부
최 준 용

실제 대용량 공격 로그의 직접적 분석으로 밝힌 공격형태

Features of attacks based on the direct analysis of real bulk attack logs

지도교수 박 근 수

이 논문을 공학석사학위논문으로 제출함

2014년 12월

서울대학교 대학원
전기・컴퓨터 공학부
최 준 용

최준용의 석사학위논문을 인준함

2014년 12월

위 원 장	문 병 로	(인)
부 위 원 장	박 근 수	(인)
위 원	Srinivasa Rao Satti	(인)

요 약

최근 네트워크의 관제시스템에서는 보안을 위해 다양한 종류의 장비가 이용된다. 이에 각 장비들에서 발생시키는 공격 로그들은 점점 증가하고 있고, 시스템을 운영하는 관리자는 로그들을 통합적으로 분석하여 공격에 대응해야 한다. 최근 제안되는 분석모델들은 마이닝을 통해 얻은 시그니쳐, 패턴, 통계 등을 이용하여 향후의 공격탐지를 더 정확하고 빠르게 하는데 초점이 맞춰져 있고, 가상의 환경에서 주로 실험되었다. 한편, 실제의 로그 데이터가 존재할 때에는 마이닝 기법을 적용하여 패턴을 찾는 것 이외에도 실제로 해당 네트워크에서 일어난 공격들의 공격자, 피해자, 형태 등에 대한 직접적 정보를 분석할 수 있다. 이러한 직접적 정보는 관리자에게 직관적으로 이해될 수 있어 상황을 파악하는데 유용하다. 이를 위해 본 논문에서는 실제 네트워크의 관제시스템의 5 가지 공격 로그들에 대한 직접적인 분석방법을 제시하고 적용하여 네트워크에서 일어난 주요한 공격들의 형태와, 로그 사이의 연관성에 대해서 분석하였다. 먼저 특정 로그에 대해 공격유형 분석을 진행하고 공격 그래프를 제안하여 분석범위를 전체에 대해 확장하였다. 또한 로그들의 연관성에 대해서도 단계별로 분석하였다. 그 결과, 네트워크에서 일어난 주요한 공격의 형태와 로그 간 연관성에 대해서 파악할 수 있었다.

주요어 : 네트워크, 실제 로그, 직접적 분석, 공격 유형, 그래프, 연관성
학번 : 2013-20897

목차

1. 서론 ····· 1

2. 로그데이터 ····· 4

3. 특정 로그에 대한 구체적 분석방법과 그 결과 ····· 5

4. 로그 기반의 공격 그래프
 4. 1 로그 기반의 공격 그래프의 정의 ····· 11
 4. 2 IXDDOS와 TMS의 공격 그래프 ····· 12
 4. 3 공격 그래프(IXDDOS, TMS)의 in/out degree 분포 ····· 13
 4. 4 공격 그래프(IXDDOS, TMS)의 시각화 ····· 15

5. 로그 사이의 연관성 ····· 17

6. 결론 ····· 25

참고 문헌 ····· 26

Abstract ····· 30

1. 서론

바이러스, 악성코드, 서비스 거부 공격(DOS) 등의 증가로 네트워크의 관제시스템은 보안장비를 이용하여 발생하는 여러 공격들을 탐지해 대응한다. 과거 단순한 경로로 이루어지던 공격들에 대해서는 소수의 보안장비로 그 역할을 충분히 해내었지만, 현재의 공격들은 매우 다양하고 복잡해져서 해결방법이 필요하다. 이러한 상황에 대응한 최근의 추세는 관제시스템에 여러 장비를 두어 장비 별로 특정한 역할만 수행하도록 하는 것이다[1]. 이렇게 함으로써 더 세밀하게 정보를 수집하고 대응할 수 있기 때문이다.

이러한 관제시스템은 구조와 공격탐지 기법에 따라서 각각 두 가지로 분류된다. 먼저 관제시스템은 구조에 따라 Network-based System과 Host-based System으로 구분된다[20]. Network-based System은 해당 네트워크에 속한 모든 host를 관찰하기 좋은 지점들에 감시시스템을 설치하고 네트워크의 트래픽을 관찰하여 이상 징후가 감지되면 이를 공격으로 탐지한다. 들어오고 나가는 모든 트래픽을 관찰하는 것이 가장 이상적이지만 이는 네트워크의 성능을 떨어트려 병목이 될 수 있어 Trade-off가 존재한다. Host-based System은 각각의 호스트에서 동작하는 것으로 해당 호스트의 네트워크 트래픽, 시스템로그, 활동, 명령어 등을 살펴서 이상 징후가 감지되면 공격으로 탐지하고 관리자에게 알린다. 또한 관제시스템은 공격을 탐지하는 기법에 따라 Signature-based Detection과 Statistical Anomaly Detection으로 구분된다. Signature-based Detection은 잘 알려진 Anti-virus System과 유사하게 동작하는 것인데, 이미 알려진 공격 행위의 시그니쳐들을 데이터베이스화 해놓고 이를 공격탐지에 이용하는 것이다. 이 방법의 약점은 데이터베이스에 없는 공격들은 탐지할 수 없다는 것이다. Statistical

Anomaly Detection은 호스트의 활동패턴을 살펴 이전에 통계적으로 얻은 정상패턴을 벗어나면 공격이라고 탐지하는 것이다. 이렇게 탐지된 것은 실제 공격일 수도 있고 아닐 수도 있는 잠재적인 공격인데 이 때문에 공격을 정확하게 탐지하는 것이 어렵다. Signature-based Detection과는 다르게 사전에 공격이라고 알려진 시그니쳐의 정보가 필요하지 않아서, 알려지지 않은 공격을 탐지하는 경우 더 유용하다[18-20].

하지만 현실에서 이러한 방법을 사용하여 공격에 대응할 때 문제가 발생한다. 시스템에서 아주 많은 양의 공격 로그가 발생되는데[2][3] 이중의 상당수가 중요하지 않은 공격 로그이거나, 잘못 탐지된 공격 로그이기 때문이다[3-8]. 이러한 이유 때문에 공격 로그를 처리하여 분석하는 기술이 광범위하게 연구되었다[2-21]. 특히 클러스터링과 데이터 마이닝을 기반으로 하는 방법들이 자주 제안되었는데 이들은 과거의 공격 로그들에서 마이닝으로 얻은 규칙이나 수치를 공격 탐지에 이용하였다. R. Vaarandi는 데이터마이닝 기법을 이용하여 전체 공격로그에서 중요한 공격 로그만 분류하는 방법을 제안하였다[3][4]. Julisch and Dacier는 공격 로그들을 클러스터링 하여 실제 공격 로그의 특성을 얻고, 이를 향후의 필터링이나 연관성을 찾는데 이용하는 방법들을 제안했다[5-7]. Treinen and Thurimella는 공격의 종류별로 해당 공격을 탐지하는데 쓰이는 마이닝 규칙을 제안하였다[8]. Clifton and Gengo도 비슷한 방식으로 접근하여 잘못 탐지한 로그를 필터링하는 방법을 제안하였다[10]. Schwartz and Stoecklin는 Snort 로그를 대상으로 클러스터링 하여 실제 공격 로그와 잘못 탐지한 로그를 구별하는 알고리즘을 제안하였다[9]. Al-Mamory, Zhang and Abbas는 클러스터링을 통해 공격 로그들을 일반화하여 이를 필터링에 이용하였다[11][12]. Pietraszek는 머신러닝을 이용하여 공격 로그를 분류하고 이를 이용하여 잘못 탐지한 로그들을 필터링 하였다[13]. Viinikka는 대

용량 공격 로그들의 시계열 분석을 통해 로그들에 적용되는 규칙을 모델링하여 중요하지 않거나 잘못 탐지된 로그를 찾아내었다[14]. P. Ning, Y. Cui, and D. S. Reeves는 그래프에 기반을 두어 공격 로그 사이의 연관성을 찾는 방법을 제안하였다[15].

최근에는 처리속도에 대한 이슈로도 연구방향이 확대되었는데, 대용량의 공격 로그 처리를 위해서 Hadoop을 이용한 분석방법들이 제안되었다[16-18]. 또한 새로운 접근법으로 Takayuki Itoh et al. 은 공격 로그들의 IP주소에 따라 전체 로그정보를 계층적으로 시각화하여 시스템의 관리자가 직관적인 판단을 내리는데 도움을 주는 방법을 제안하였다[21].

이처럼 로그정보는 갈수록 증가하는 상황에서 이를 통합적으로 분석하여 한 차원 위에서 공격을 탐지하고 대응하는 것이 최근의 모델로 제안되고 있다. 이러한 모델들은 마이닝을 통해 얻어낸 시그니쳐, 패턴, 통계 등을 이용하여 향후의 공격탐지를 더 정확하고 빠르게 하는 것에 초점이 맞춰져 있고 가상의 환경에서 주로 실험되었다. 한편, 실제의 로그 데이터가 존재할 때에는 마이닝 기법을 적용하여 패턴을 찾는 것 이외에도 실제로 해당 네트워크에서 일어난 공격들의 공격자, 피해자, 형태 등에 대한 직접적 정보를 분석할 수 있다. 이러한 직접적 정보는 관리자에게 직관적으로 이해될 수 있어 상황을 파악하는데 유용하다. 이를 위해 본 논문에서는 실제 네트워크의 관제시스템의 5 가지 공격 로그들에 대한 직접적인 분석방법을 제시하고 적용하여 네트워크에서 일어난 주요한 공격들의 형태와, 로그 사이의 연관성에 대해서 분석하였다.

2. 로그데이터

분석할 데이터는 30일 동안 기록된 서로 다른 5종류의 로그파일들이다. 각 로그들은 실제 네트워크 관제시스템에서 운영하는 서로 다른 보안장비들에서 기록된다. IXDDOS와 TMS는 실제 공격을 탐지한 것에 대한 로그이고 그 형식이 같다. MCF는 악성 URL의 탐지에 관련된 로그인데 두 개의 IP와 URL을 갖는다. 이때 두 IP 중 먼저 나오는 IP는 URL의 실제 IP와 같다. RBL은 스팸메일의 탐지에 관련된 로그이고, DNSSINK는 DNS의 접속기록과 관련된 로그이다. 모든 로그에는 Time, IP에 대한 정보가 있고, 장비의 종류에 따라 추가 정보를 갖는다. 로그들의 분석을 위해 먼저 각 로그별로 파일 크기, 총 로그의 개수, 총 IP의 개수를 조사하여 로그들의 대략적인 규모를 파악하였다. 이에 대한 결과는 [표 1]과 같다.

[표 1] 로그별 수치 데이터

	File Size	Total Line	Distinct IP
IXDDOS	455MB	11,243,398	1,647,240
TMS	558MB	12,712,530	220,514
MCF	3.69GB	78,615,927	14,736
RBL	4.02GB	64,052,686	1,528,582
DNSSINK	765MB	11,597,406	159,999

3. 특정 로그에 대한 구체적 분석방법과 그 결과

이어서 5가지 로그 중 공격에 대한 로그들(IXDDOS, TMS)에 대해 구체적인 분석을 진행하였다. 두 로그의 형식이 완전히 같고, 실제 공격을 탐지한 로그라는 점에서 다른 로그들보다 분석에 용이하기 때문이다.

한 로그에 대한 구체적 분석과정은 공격받은 횟수, 공격한 횟수를 기반으로 진행된다. 먼저 IP 별로 공격받은 횟수를 조사하여 내림차순으로 정렬 후, 최상위 IP 30개에 대해 해당 IP를 공격한 Src(Source) IP들이 각각 어떤 공격들을 몇 번씩 했는지 조사하여 내림차순으로 정렬한다. 각 Src IP에서 행해진 공격종류들의 구체적인 작동방법에 따라서 공통점이나 패턴을 찾고, Src IP간에 이를 비교하여 일관성 있게 찾아진 공통점이나 경향성은 해당 Src IP들과 Dst(Destination) IP 간에 이뤄진 공격들을 대표할 수 있다. 또한 공격한 횟수를 기반으로 위 과정의 Src IP와 Dst IP를 서로 바꾸어 같은 방식으로 분석한다. IXDDOS와 TMS에 대한 분석결과는 [표 2, 4, 5, 6]과 같다.

다음 [표 2]는 IXDDOS를 위의 방법으로 조사하여 그 중 가장 공격을 많이 받은 IP인 xxx.217.247.100에 대해 정리한 표이다. 표의 3, 4번째 열은 해당 IP를 공격한 Src IP중 가장 많이 공격한 xxx.111.39.167이 수행한 공격의 종류와 그 횟수이다.

[표 2] IXDDOS 중 가장 공격을 많이 받은 IP

xxx.217.247.100 (총 2,291,326 번 공격받음)			
Src IP(727,014개)	count	xxx.111.39.167	count
xxx.111.39.167	**20,689**	TCP-Connect-DOS	7,594
xxx.94.41.89	12,462	TCP-ACK-Flooding	7,497
xxx.238.13.207	11,159	TCP-FIN-Flooding	5,521
xxx.76.225.121	11,093	TCP-SYN-Flooding(DDoS)	77
xxx.238.13.205	10,901		
xxx.141.0.80	8,423		
xxx.220.221.163	7,982		
xxx.94.207.66	7,584		
xxx.216.80.50	7,186		
xxx.90.135.156	6,683		

xxx.217.247.100은 xxx.111.39.167에게 가장 많은 공격(20,689번)을 받았다. 공격은 특정 동작을 요구하는 패킷들을 대량으로 보내 Dst IP에서 해당 동작을 하도록 요청하여 자원을 낭비시키는 방식이었다. xxx.111.39.167을 제외한 나머지 상위 9개 Src IP들의 공격들도 서비스 거부를 유발하는 것들이 주류임을 확인하였다.

또한 IXDDOS 상에서 xxx.217.247.100이 받은 공격의 종류는 총 16가지이고 그 중 상위 10개의 종류와 각 횟수는 [표 3]과 같다. 네트워크상에서 xxx.217.247.100이 받은 모든 공격들은 그 IP를 주도적으로 공격한 Src IP들의 공격 형태와 유사했다.

[표 3] xxx.217.247.100이 받은 전체 공격의 종류와 수

xxx.217.247.100	
Attack type	count
TCP-Connect-DOS	2,013,187
TCP-ACK-Flooding	255,177
TCP-SYN-Flooding(DDoS)	11,765
TCP-FIN-Flooding	8,186
TCP-RST-Flooding	1,632
TCP-SYN-Flooding	543
HTTP-Cache-Control-Request-Flooding-3	371
TCP-Tear-Drop	225
TCP-Invalid-flags-(maerong)	180
HTTP-Main-Page-Request-Flooding	43

다음 [표 4]는 IXDDOS를 위의 방법으로 조사하여 그 중 공격을 가장 많이 수행한 IP인 xxx.148.1.91에 대해 정리한 표이다. 표의 3, 4번째 열은 해당 IP가 공격한 Dst IP들이 당한 공격의 종류와 그 횟수이다.

[표 4] IXDDOS 중 가장 공격을 많이 수행한 IP

xxx.148.1.91 (총 276,155번 공격함)			
DstIP(275,983개)	count	Attack	count
xxx.234.231.139	2	Win32/Slamer.Worm-1-(UDP-1434)	276,155
xxx.179.162.5	2		
xxx.228.88.128	2		
xxx.178.197.246	2		
xxx.177.251.46	2		
xxx.176.251.5	2		
xxx.177.200.93	2		
xxx.35.208.33	2		
xxx.177.197.20	2		
xxx.160.19.98	2		

xxx.148.1.91은 IXDDOS 상에서 가장 많은 공격(276,155번)을 수행했지만, 공격방식은 한 가지로 이루어졌다. 또한 특정 IP를 집중적으로 공격하지 않고 매우 다양한 IP(275,983개)를 최대 두 번 공격하였다. 해당 공격은 메모리 상주 Worm의 한 종류로써 공격대상에게 버퍼오버플로우를 일으켜 정상적인 작동을 불가능하게 만드는 것이다.

다음 [표 5]는 TMS를 위의 방법으로 조사하여 그 중 가장 공격을 많이 받은 IP인 xxx.61.16.22에 대해 정리한 표이다. 표의 3, 4번째 열은 해당 IP를 공격한 Src IP들이 수행한 공격의 종류와 그 횟수이다.

[표 5] TMS 중 가장 공격을 많이 받은 IP

xxx.61.16.22 (총 22,384번 공격 받음)			
SrcIP (886개)	count	Attack	count
xxx.97.84.1	123	TCP-Connect-DOS	22,384
xxx.97.87.1	122		
xxx.97.93.1	122		
xxx.97.87.254	119		
xxx.97.82.1	119		
xxx.97.84.254	118		
xxx.97.85.254	118		
xxx.97.88.1	114		
xxx.97.94.199	76		
xxx.97.82.29	73		

xxx.61.16.22은 xxx.97.84.1에게 가장 많은 공격(123번)을 받았다. 받은 공격은 모두 서비스 거부를 일으키는 TCP-Connect-DOS 인데 이는 IXDDOS에서 가장 많이 공격받은 IP가 받은 공격 중 하나와 같다 [표 2].

다음 [표 6]은 TMS를 위의 방법으로 조사하여 그 중 공격을 가장 많이 수행한 IP인 xxx.175.243.22에 대해 정리한 표이다. 표의 3, 4번째 열은 해당 IP가 공격한 Dst IP들이 당한 공격의 종류와 그 횟수이다.

[표 6] TMS 중 가장 공격을 많이 수행한 IP

xxx.175.243.22 (총 242,778번 공격함)			
DstIP (448개)	count	Attack	count
xxx.251.47.213	1,943	TCP-Invalid-flags-(maerong)	242,728
xxx.251.40.168	1,943	Host-Sweep	50
xxx.251.89.150	1,943		
xxx.251.80.125	1,943		
xxx.251.43.72	1,943		
xxx.251.118.86	1,942		
xxx.251.91.145	1,942		
xxx.251.36.192	1,942		
xxx.251.114.109	1,942		
xxx.251.122.62	1,942		

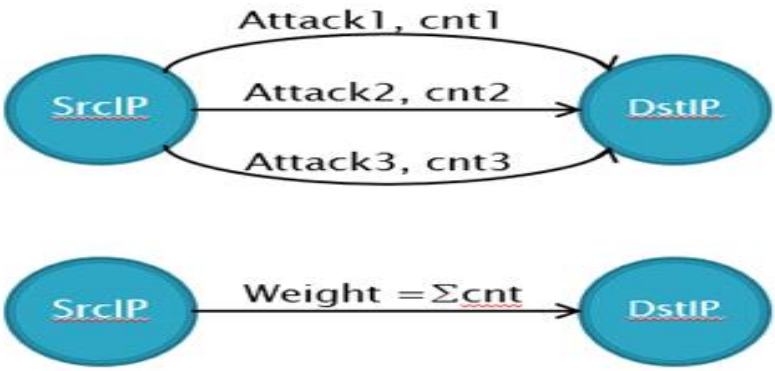
xxx.175.243.22은 TMS 상에서 가장 많은 공격(242,778번)을 수행했고 공격방식은 주로 TCP-Invalid-flags-(maerong) 한가지였다. 해당 공격은 네트워크의 관제시스템이 운영되는 서버에 공격으로 해석될 만한 패킷들을 다량 전송하는 것으로, 시스템이 오탐하도록 혼동을 주어서 서비스 거부를 일으킨다.

4. 로그 기반의 공격 그래프

4.1 로그 기반의 공격 그래프 정의

앞의 방식은 로그에 많이 등장한 중요 IP들의 공격 형태에 대해 집중하여 분석할 수 있었지만, 모든 IP를 포함하여 전체적인 관점에서 분석하기 어렵다. 이를 해결하고자 본 논문에서는 로그 기반의 공격 그래프를 정의하여 IP 전체에 대한 효과적인 분석방법을 제시하였다.

새로 정의한 그래프[그림 1]는 방향성 그래프이고 정점과 간선의 정의는 다음과 같다. 정점은 로그에 등장한 Src/Dst IP이고, 같은 IP들은 한 개의 정점으로 대응된다. 두 정점 간에는 공격의 종류별로 가상의 간선을 가질 수 있고, 이때 그 간선의 가중치는 해당 공격의 횟수이다. 정점 간의 실제 간선은 한 개이고 그 가중치는 존재하는 가상 간선들의 가중치 합이다.



[그림 1] 로그 기반 공격 그래프의 정의

4.2 IXDDOS와 TMS의 공격 그래프

본 논문에서는 정의한 그래프를 IXDDOS와 TMS에 적용하고 그래프에 나타난 특징들을 분석하였다. 먼저 4단계로 간선 가중치의 임계값(1000, 100, 10, 0)을 설정하고, 임계값 이상인 간선들로 이루어진 그래프에 대하여 각각 여러 수치 값들을 조사하여 그래프의 대략적인 모습을 파악했다. 이는 정점의 수, 간선의 수, 간선들의 가중치 평균, 각 정점의 indegree 평균, 각 정점의 outdegree 평균, 파티션의 개수를 구하여 알아보았다. IXDDOS와 TMS에서 구한 값들은 [표 7], [표 8]과 같다.

[표 7] IXDDOS의 단계별 그래프에 대한 수치 값

W bound	V	E	Indeg	Outdeg	Weight	Partition
1,000	281	220	1.65	1.43	2955.96	71
100	2,877	2,601	2.22	1.48	477.02	497
10	26,384	57,176	6.12	1.21	41.78	3,735
0	1,647,240	2,021,367	3.97	1.76	2.78	26,829

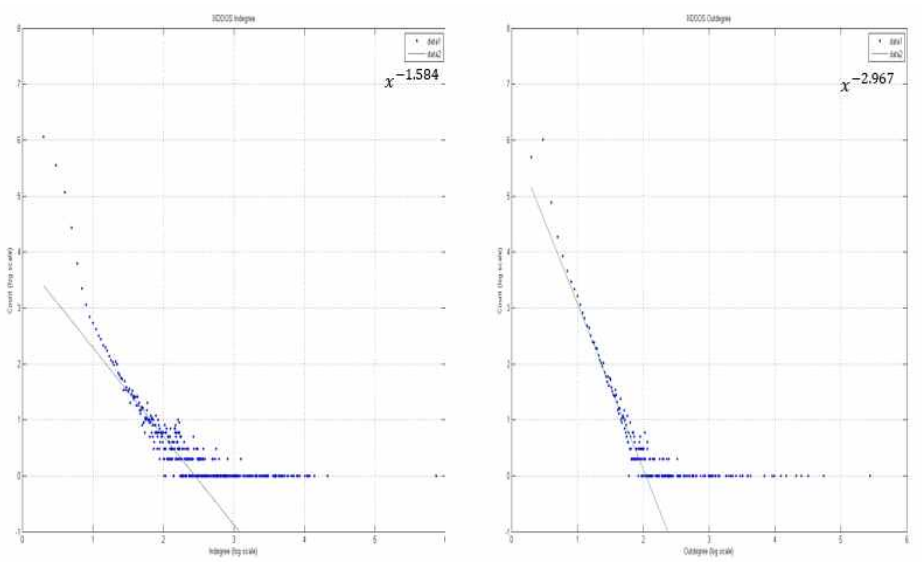
[표 8] TMS의 단계별 그래프에 대한 수치 값

W bound	V	E	Indeg	Outdeg	Weight	Partition
1,000	136	132	1.01	18.85	2103.47	5
100	311	667	2.85	7.57	772.17	34
10	20,614	88,459	5.07	22.51	20.25	179
0	220,514	952,135	19.03	21.75	2.47	7

임계값을 낮춰가며 그래프를 확장했을 때 IXDDOS의 평균 outdegree는 2이하의 값들을 가졌고, TMS에서는 임계값에 따른 평균 outdegree가 17정도의 값을 가졌다.

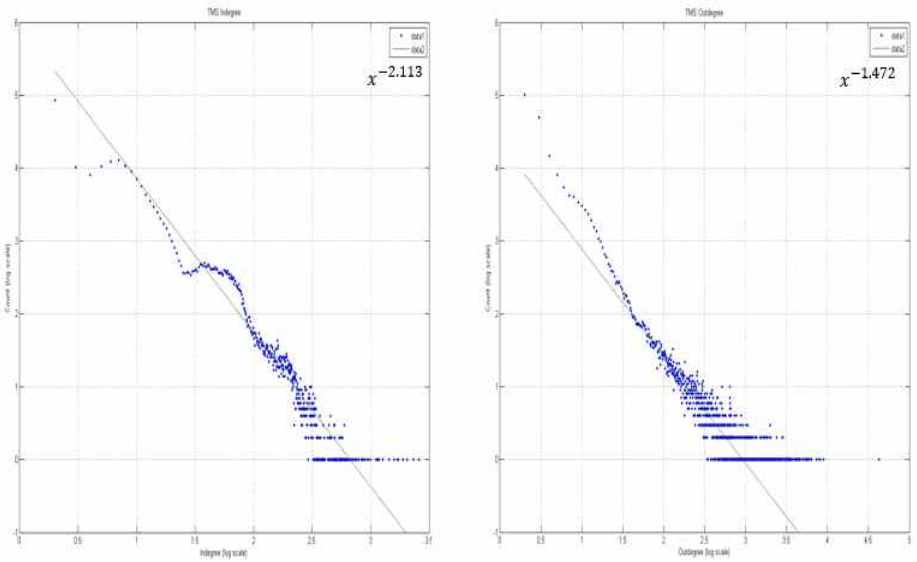
4.3 공격 그래프(IXDDOS, TMS)의 in/out degree 분포

다음으로 IXDDOS와 TMS의 in/out degree에 대한 분포를 분석하였다. 구체적인 degree 분포에 대한 정보로 공격 형태를 좀 더 자세히 알아낼 수 있기 때문이다. [그림 2], [그림 3]은 IXDDOS와 TMS의 in/out degree에 대한 분포 그래프이다. 그래프의 가로축은 in(좌)/out(우) degree이고 세로축은 해당 차수를 가지는 정점의 수이다. 각 축은 모두 밑이 10인 로그스케일로 표시되어 있다.



[그림 2] IXDDOS의 in(좌)/out(우) degree에 대한 분포

[그림 2]의 IXDDOS indegree 분포 그래프를 살펴보면 낮은 degree를 지닌 정점이 굉장히 많고, 높은 degree를 지닌 정점은 매우 적음을 알 수 있다. 이는 다수의 IP에게 공격받은 IP의 수가 매우 적다고 할 수 있는데, 다수에 의한 분산 공격이 주로 소수에게 집중적으로 일어남을 알 수 있다. 이러한 분포는 Y = C * X + k , X = 가로축 값, Y = 세로축 값, C = -1.584 를 갖는 식으로 근사시킬 수 있는데 이는 결과지수 -1.584를 갖는 멱법칙[23]을 따름을 확인할 수 있었다. [그림 2]의 outdegree 그래프도 낮은 degree를 지닌 정점이 굉장히 많고 높은 degree를 지닌 정점은 매우 적었는데 위의 수식에서 C가 -2.967인 경우로 근사시킬 수 있었고 이 역시 결과지수 -2.967을 갖는 멱법칙을 따랐다[22].

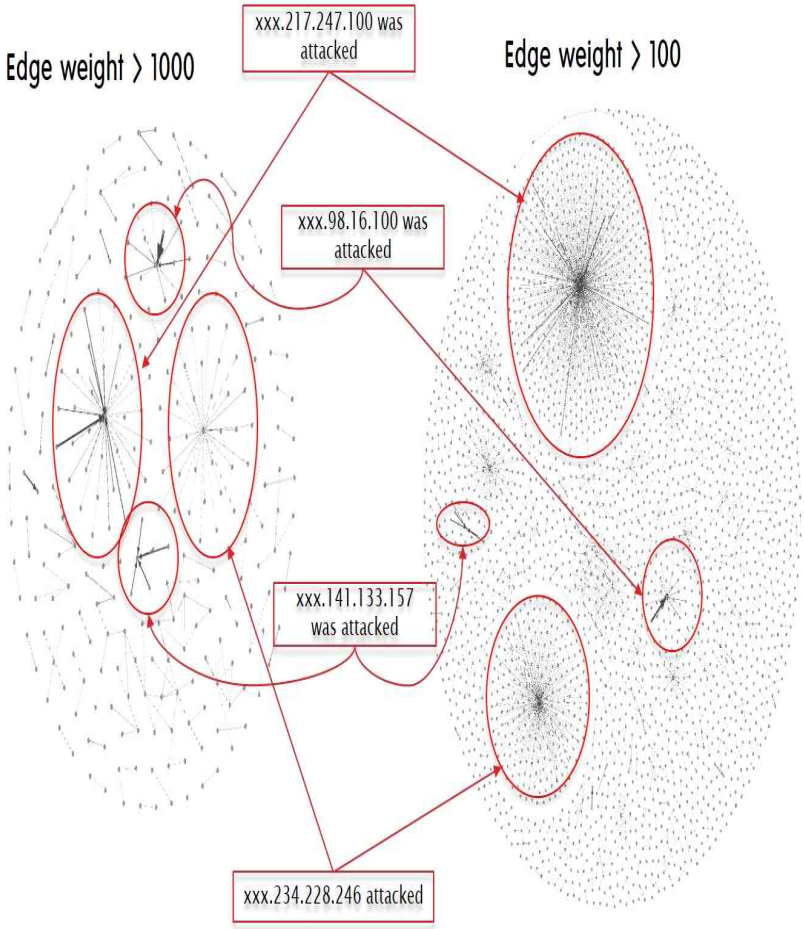


[그림 3] TMS의 in(좌)/out(우) degree에 대한 분포

[그림 3]의 TMS in/out degree 분포 그래프도 각각 -2.113, -1.472의 C값을 갖는 수식으로 근사시킬 수 있었고, 해당 C값을 결과지수로 가지는 멱법칙을 따랐다.

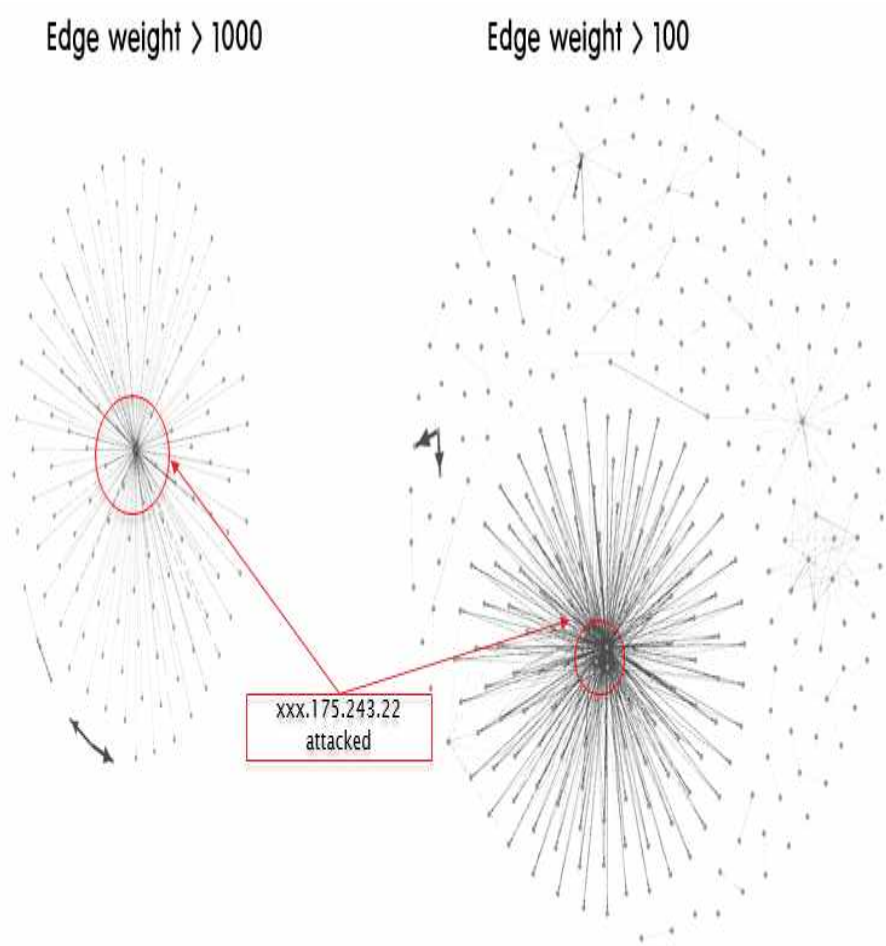
4.4 공격 그래프(IXDDOS, TMS)의 시각화

또한 가중치가 1000, 100이상인 간선으로 구성된 IXDDOS와 TMS의 공격 그래프들을 Graph Visualization Tool인 Gephi[24]를 이용하여 시각화하였다[그림 4][그림 5]. IXDDOS에서 간선의 가중치가 1000이상인 경우 몇몇 클러스터가 이루어졌고, 이를 확장했을 때 해당 클러스터들의 중심점들이 유지되며 클러스터가 확장되었다. 클러스터에 해당하지 않는 노드들 간의 연결은 매우 적었다.



[그림 4] 로그 IXDDOS에 대한 공격 그래프

TMS에서는 간선의 가중치가 1000이상인 경우 하나의 클러스터가 이루어졌고, 이를 확장했을 때 IXDDOS와 유사하게 해당 클러스터의 중심에 몇 개의 노드가 추가되며 클러스터가 확장되었다. 반면 IXDDOS와는 다르게 TMS는 클러스터 외에도 여러 개의 partition들이 존재하여 더 복잡한 형태를 가졌다.



[그림 5] 로그 TMS에 대한 공격 그래프

5. 로그 사이의 연관성

특정 로그들을 개별적으로 분석한 이후, 로그 간 연관성에 대해 2단계로 조사를 진행하였다. 먼저 로그별로 서로 교집합 되는 IP들의 수를 조사하였고 결과는 [표 5]와 같다.

[표 5] 로그별 IP 교집합 수

	TMS	MCF	RBL	DNSSINK
IXDDOS	2,381	1,085	6,656	14,774
TMS	-	40	1,817	497
MCF	-	-	960	46
RBL	-	-	-	2,753

교집합인 IP들의 비율은 비교한 두 로그 중 IP 수가 더 많은 것을 기준으로 모두 1% 미만의 작은 값이었다. 하지만 교집합인 IP의 개수가 적더라도 이들이 관여한 로그의 수가 많다면 두 로그 사이의 연관성이 존재한다고 할 수 있으므로 그에 대한 조사를 다음 단계로 진행하였다.

다음 단계에서는 공격 로그인 IXDDOS, TMS에 대해 Src IP, Dst IP를 구분하여 각각 가장 많이 등장한 IP를 30개씩 선택하고, 선택된 IP들이 다른 로그들에 몇 개가 나타는지 조사하였다.

조사 결과, IXDDOS의 Src IP로 많이 등장했던 IP 중 4개가 TMS에서 Src IP로 검출되거나 MCF에서 검출되었고 IXDDOS의 Dst IP로 많이 등장했던 IP 중 2개가 TMS의 Src IP로 검출되거나 MCF에서 검출되었다. 또한 TMS의 Dst IP로 많이 등장했던 IP 중 1개가 IXDDOS의 Dst IP로 검출되었다. 이로 미루어 로그들 사이에 연관성이 있음을 알 수 있다. 다음 표들은 위의 검출된 IP들이 양쪽 로그에서 어떤 형태로 나타나는지 정리한 것이다.

[표 6], [표 7]은 검출한 것 중 IXDDOS의 Src IP로 많이 등장한 IP인 xxx.61.11.248이 TMS의 Src IP에서 나타난 경우에 대해 각 로그에서 해당 IP가 공격한 Dst IP와 공격 종류를 정리한 표이다.

[표 6] IXDDOS에서 xxx.61.11.248의 공격형태

xxx.61.11.248 (IX_src)			
DstIP (11,073)	count	Attack	count
xxx.111.117.192	137	TCP-Invalid-port	15,903
xxx.109.212.136	134	TCP-SYNACK-Flooding	148
xxx.231.157.93	134		
xxx.55.127.199	133		
xxx.112.78.246	130		
xxx.122.206.86	129		
xxx.98.67.143	129		
xxx.231.65.10	129		
xxx.35.242.156	127		
xxx.248.11.3	127		

[표 7] TMS에서 xxx.61.11.248의 공격형태

xxx.61.11.248 (TMS_src)			
DstIP (524)	count	Attack	count
xxx.172.86.128	54	TCP-Invalid-flags-(maerong)	509
xxx.172.160.205	48	TCP-DRDOS-Attack	374
xxx.37.235.174	47		
xxx.233.249.179	47		
xxx.98.214.140	45		
xxx.219.24.105	39		
xxx.237.203.87	36		
xxx.172.175.196	27		
xxx.221.185.92	21		
xxx.37.231.87	3		

[표 8], [표 9]는 검출한 것 중 IXDDOS의 Src IP로 많이 등장한 IP인 xxx.0.0.0이 TMS의 Src IP에서 나타난 경우에 대해 각 로그에서 해당 IP가 공격한 Dst IP와 공격 종류를 정리한 표이다. [표 10]은 xxx.0.0.0이 MCF의 2st IP로 나타난 경우에 대해 해당 로그에 포함된 URL IP와 URL의 등장횟수를 정리한 표이다.

[표 8] IXDDOS에서 xxx.0.0.0의 공격형태

xxx.0.0.0 (IX_src)			
DstIP (992)	count	Attack	count
xxx.0.0.0	5369	Total_traffic_rate_Misuse	7,538
xxx.239.123.121	714	System-Info	4,477
xxx.53.115.33	659	TCP_SYN_Misuse	4,281
xxx.53.115.34	620	Bandwidth	549
xxx.53.99.16	594	Protocol	343
xxx.53.117.25	586	ICMP_Misuse	293
xxx.238.14.59	487	IP-Invalid-Address	225
xxx.53.114.24	473	Private_IP_address_Misuse	192
xxx.53.114.12	471	IP_Fragment_Misuse	162
xxx.238.12.247	453	TCP_RST_Misuse	139

[표 9] TMS에서 xxx.0.0.0의 공격형태

xxx.0.0.0 (TMS_src)			
DstIP (7)	count	Attack	count
xxx.251.128.201	30	IP-Invalid-Address	36
xxx.220.57.105	1		
xxx.115.23.96	1		
xxx.233.248.170	1		
xxx.97.89.24	1		
xxx.251.137.219	1		
xxx.220.57.105	1		

[표 10] MCF에서 xxx.0.0.0의 로그형태

xxx.0.0.0 (MCF의 2st IP)		
URL IP (1)	count	URL
xxx.45.144.166	719	http://xxxxxx.com/hanil/index.html

[표 11], [표 12]은 검출한 것 중 IXDDOS의 Src IP로 많이 등장한 IP인 xxx.164.132.118이 TMS의 Src IP에서 나타난 경우에 대해 각 로그에서 해당 IP가 공격한 Dst IP와 공격 종류를 정리한 표이다.

[표 11] IXDDOS에서 xxx.164.132.118의 공격형태

xxx.164.132.118 (IX_src)			
DstIP(1,266)	count	Attack	count
xxx.216.115.237	96	TCP-Invalid-port	10,496
xxx.216.1.109	51		
xxx.216.59.215	50		
xxx.228.84.111	50		
xxx.216.122.174	50		
xxx.216.110.87	50		
xxx.228.68.155	50		
xxx.216.76.150	50		
xxx.234.231.210	50		
xxx.216.81.66	50		

[표 12] TMS에서 xxx.164.132.118의 공격형태

xxx.164.132.118 (TMS_src)			
DstIP (1,089)	count	Attack	count
xxx.98.216.20	3	Host-Sweep	1,152
xxx.116.168.65	3		
xxx.238.208.80	3		
xxx.98.194.117	2		
xxx.221.191.203	2		
xxx.221.176.125	2		
xxx.237.201.134	2		
xxx.238.212.82	2		
xxx.253.125.129	2		
xxx.221.185.227	2		

[표 13], [표 14]은 검출한 것 중 IXDDOS의 Src IP로 많이 등장한 IP인 xxx.251.226.14가 TMS의 Src IP에서 나타난 경우에 대해 각 로그에서 해당 IP가 공격한 Dst IP와 공격 종류를 정리한 표이다.

[표 13] IXDDOS에서 xxx.251.226.14의 공격형태

xxx.251.226.14 (IX_src)			
DstIP (9,658)	count	Attack	count
xxx.34.150.251	3	UDP-Invalid-Data-Size	9,761
xxx.178.75.113	2		
xxx.216.189.202	2		
xxx.178.226.46	2		
xxx.216.50.108	2		
xxx.177.17.117	2		
xxx.176.20.181	2		
xxx.35.34.34	2		
xxx.160.100.69	2		
xxx.178.75.63	2		

[표 14] TMS에서 xxx.251.226.14의 공격형태

xxx.251.226.14 (TMS_src)			
DstIP (5,797)	count	Attack	count
xxx.220.60.55	3	UDP-Invalid-Data-Size	5,948
xxx.93.247.104	3		
xxx.251.143.17	3		
xxx.116.162.238	3		
xxx.238.208.157	3		
xxx.237.194.149	2		
xxx.35.113.12	2		
xxx.37.231.97	2		
xxx.98.208.134	2		
xxx.98.199.224	2		

[표 15], [표 16]은 검출한 것 중 IXDDOS의 Dst IP로 많이 등장한 IP인 xxx.205.241.24가 TMS의 Src IP에서 나타난 경우에 대한 것으로, [표 15]는 IXDDOS에서 해당 IP를 공격한 Src IP와 공격 종류를 정리한 것이고, [표 16]은 TMS에서 해당 IP가 공격한 Dst IP와 공격 종류를 정리한 것이다.

[표 15] IXDDOS에서 xxx.205.241.24가 받은 공격형태

xxx.205.241.24 (IX_dst)			
SrcIP (11,073)	count	Attack	count
xxx.230.232.100	217	TCP-Connect-DOS	17,253
xxx.141.117.149	138	TCP-ACK-Flooding	111
xxx.32.112.72	53	ICMP-Source-IP-Flooding	24
xxx.148.50.154	45	ICMP-Destination-IP-Flooding	3
xxx.141.117.139	41	TCP-RST-Flooding	2
xxx.35.27.183	40	TCP-FIN-Flooding	1
xxx.141.100.66	40		
xxx.141.100.88	39		
xxx.141.100.61	32		
xxx.141.117.173	30		

[표 16] TMS에서 xxx.205.241.24의 공격형태

xxx.205.241.24 (TMS_src)			
DstIP (3)	count	Attack	count
xxx.37.228.57	1	Host-Sweep	3
xxx.97.95.112	1		
xxx.97.83.137	1		

[표 17], [표 18]은 검출한 것 중 IXDDOS의 Dst IP로 많이 등장한 IP인 xxx.145.28.200이 MCF의 두 IP중 URL과 같은 IP로 나타난 경우에 대한 것으로, [표 17]은 IXDDOS에서 해당 IP를 공격한 Src IP와 공격종류를 정리한 것이고 [표 18]은 MCF에서 해당 IP가 등장하는 로그에 포함된 2st IP와 URL의 등장 횟수를 정리한 것이다.

[표 17] IXDDOS에서 xxx.145.28.200가 받은 공격형태

xxx.145.28.200 (IX_dst)			
SrcIP (21,168)	count	Attack	count
xxx.248.189.1	3633	TCP-Connect-DOS	68,385
xxx.216.137.7	2242	TCP-ACK-Flooding	21,581
xxx.182.190.136	883	TCP-FIN-Flooding	60
xxx.50.21.24	625	HTTP-Connection-Limit-Exhaustion-Attack (By-Slowloris)	15
xxx.247.147.132	503	TCP-RST-Flooding	15
xxx.92.127.129	494	HTTP-Transaction-Flooding(GET)	6
xxx.230.133.140	434	ICMP-Unreachable-Storm	3
xxx.120.75.254	333	TCP-SYN-Flooding	3
xxx.96.167.254	270	HTTP-Bulk-Transaction-Flooding	2
xxx.247.145.52	231	ICMP-Source-IP-Flooding	2

[표 18] MCF에서 xxx.145.28.200의 로그형태

xxx.145.28.200 (MCF의 IP 중 URL과 같은 IP)		
2st IP	count	URL
--	2,876	http://www.xxxxxx.com/dhtm/js/

[표 19], [표 20]은 검출한 것 중 TMS의 Dst IP로 많이 등장한 IP인 xxx.61.16.22가 IXDDOS의 Dst IP에서 나타난 경우에 대해 각 로그에서 해당 IP를 공격한 Src IP와 공격 종류를 정리한 표이다.

[표 19] TMS에서 xxx.61.16.22가 받은 공격형태

xxx.61.16.22 (TMS_dst)			
SrcIP (886)	count	Attack	count
xxx.97.84.1	123	TCP-Connect-DOS	22,384
xxx.97.87.1	122		
xxx.97.93.1	122		
xxx.97.87.254	119		
xxx.97.82.1	119		
xxx.97.84.254	118		
xxx.97.85.254	118		
xxx.97.88.1	114		
xxx.97.94.199	76		
xxx.97.82.29	73		

[표 19] IXDDOS에서 xxx.61.16.22가 받은 공격형태

xxx.61.16.22 (IX_dst)			
SrcIP (16)	count	Attack	count
xxx.30.151.161	5	ICMP-Destination-IP-Flooding	23
xxx.115.193.124	2		
xxx.115.197.188	2		
xxx.110.55.9	2		
xxx.30.147.33	1		
xxx.30.157.206	1		
xxx.30.197.189	1		
xxx.30.246.91	1		
xxx.30.250.157	1		
xxx.228.207.18	1		

6. 결론

본 논문에서는 네트워크 관제시스템에 속한 서로 다른 5 종류의 보안 장비에서 기록된 실제 대용량 로그파일에 대해 몇 가지 분석 방법을 제안하여 적용하였다. 그 결과, 공격을 주도하는 IP들의 공격 형태를 파악할 수 있었고, 공격 그래프를 통해 분석 범위를 전체 IP로 확장하였다. 또한 단계별로 로그사이에 IP 교집합을 조사하여 로그간의 연관성을 찾았다. 이 논문은 특정한 5개의 로그에 대해 분석하였지만, IP기반의 다른 로그그룹에 대해서도 제시한 방법들을 사용할 수 있다. 네트워크 공격의 전체 과정은 대체로 잠복기를 거쳐 장기간으로 진행된다. 또한 공격을 받아 감염된 호스트가 명령을 받아 다른 공격을 수행하기도 한다. 분석할 수 있는 로그의 양이 늘어난다면 이러한 요소들을 공격 그래프의 분석을 통해 찾아내 방어에 활용할 수 있을 것이다.

참고 문헌

[1] 정일권 et al. , “DDos 공격에 대한 효과적인 보안 관제 방안,” 한국융합보안학회 정보•보안 논문지, vol. 9, iss. 4, pp. 7-12

[2] J. Viinikka, H. Debar, L. Mé, A. Lehikoinen, and M. Tarvainen, “Processing intrusion detection alert aggregates with time series modeling,” Information Fusion Journal, vol. 10(4), 2009, pp. 312-324.

[3] R. Vaarandi, “Real-Time Classification of IDS Alerts with Data Mining Techniques,” in Proc. of 2009 MILCOM Conference, pp. 1-7

[4] Risto Vaarandi and Karkus Podins, “Network IDS alert classification with frequent itemset mining and data clustering”, Network and Service Management 2010, pp. 451-456

[5] K. Julisch, “Mining Alarm Clusters to Improve Alarm Handling Efficiency,” in Proc. of 2001 Annual Computer Security applications Conference, pp. 12-21.

[6] K. Julisch and M. Dacier, “Mining intrusion detection alarms for actionable knowledge,” in Proc. of 2002 ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 366-375.

[7] K. Julisch, “Clustering Intrusion Detection Alarms to Support Root Cause Analysis,” ACM Transactions on Information and System Security, vol. 6(4), 2003, pp. 443-471.

[8] J. J. Treinen and R. Thurimella, “A Framework for the Application of Association Rule Mining in Large Intrusion Detection Infrastructures,” in Proc. of 2006 RAID Symposium, pp. 1-18.

[9] J. Long, D. Schwartz, and S. Stoecklin, “Distinguishing False from True Alerts in Snort by Data Mining Patterns of Alerts,” in Proc. of 2006 SPIE Defense and Security Symposium, pp. 62410B-1—62410B-10.

[10] C. Clifton and G. Gengo, “Developing Custom Intrusion Detection Filters Using Data Mining,” in Proc. of 2000 MILCOM Symposium, pp. 440-443.

[11] S. O. Al-Mamory, H. Zhang, and A. R. Abbas, “IDS Alarms Reduction Using Data Mining,” in Proc. of 2008 IEEE World Congress on Computational Intelligence, pp. 3564-3570.

[12] S. O. Al-Mamory and H. Zhang, “Intrusion Detection Alarms Reduction Using Root Cause Analysis and Clustering,” Computer Communications, vol. 32(2), 2009, pp. 419-430.

[13] T. Pietraszek, “Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection,” in Proc. of 2004 RAID Symposium, pp. 102-124.

[14] J. Viinikka, H. Debar, L. Mé, and R. Séguier, “Time Series Modeling for IDS Alert Management,” in Proc. of 2006 ACM Symposium on Information, Computer and Communications Security, pp. 102-113.

[15] P. Ning, Y. Cui, and D. S. Reeves, “Analyzing Intensive Intrusion Alerts via Correlation,” in Proc. of 2002 RAID Symposium, pp. 74-94.

[16] Shun-Fa Yang, Taichung, Wei-Yu Chen, Yao-Tsung Wang, “ICAS: An inter-VM IDS Log Cloud Analysis System,” Cloud Computing and Intelligence Systems (CCIS) 2011 IEEE International Conference, pp. 285-289.

[17] 최대수 et al, “Mapreduce를 이용한 대용량 보안 로그 분석,” 한국정보기술학회논문지 2011, vol.9, iss.8, pp.125-132.

[18] Jakrarin Therdphapiyanak, Krerk Piromsopa, “Applying Hadoop for log analysis toward distributed IDS,” ICUIMC 2013, Article No. 3

[19] B. Mukherjee, L. Heberlein, and K. Levitt. “Network intrusion detection,” Network IEEE 1994, vol. 8, iss. 3, pp. 26-41.

[20] Wikipedia. Intrusion detection system, http://en.wikipedia.org/wiki/Intrusion_detection_system

[21] Takayuki Itoh, Hiroki Takakura, “Hierarchical visualization of network intrusion detection data,” Computer Graphics and Applications IEEE 2006, vol.26, issue.2, pp. 40-47.

[22] 서정주 et al, “국내 웹 그래프의 링크 구조 분석,” 정보과학회논문지 : 컴퓨팅의 실제 및 레터 2009, vol.19, iss.1, pp. 7-14.

[23] Wikipedia. Power law, http://en.wikipedia.org/wiki/Power_law

[24] Gephi, Graphic Visualization Tool, http://gephi.github.io/

Abstract

Features of attacks based on the direct analysis of real bulk attack logs

Jun Yong Choi
Department of Computer Science and Engineering
The Graduate School
Seoul National University

Recently, a network control system uses various equipments which are used to defend malicious attacks. Attack logs generated by each equipments are steadily increasing and the manager of the network control system have to make an integrated analysis of these logs for reacting to attacks. Lately proposed analysis models used mining methods to get signatures, patterns, statistics and etc. These models used these things to improve an accuracy of detections of future attacks and the related experiments were conducted under virtual environments. Meanwhile, if a real data exists, we can get not only patterns which are results of the mining methods, but also direct informations which contain attackers, victims, attack types. These things can be useful to the manager because situations of the network can be understood intuitively by that. For this purpose, we

propose the direct analysing method of attack logs and apply it to the real data. This paper proposes the method of analyzing 5 kinds of logs which are collected by security equipment of the real network control system. First of all, we analyze attack types of specific logs and extend the analysis range to entire logs by proposing the attack graph. Next, we search for correlations of different kinds of logs. As a result, we can find out the features of major attacks and correlations of logs.

Keywords : Network, Real log, Direct analysis, Attack type, Graph, Correlation

Student Number : 2013-20897