Relatório sobre o artigo “Toward developing a systematic approach to generate benchmark datasets for intrusion detection”

Gustavo Barbosa Barreto

O artigo da ISCX aborda como e porque houve a necessidade de se elaborar uma nova base de dados para testes de intrusão.
Segundo o texto até então as bases de dados existentes, eram em grande parte anonimas, não possuíam estatísticas que comprovassem quantos e quais ataques foram gerados, muito menos informações como o contexto da rede em que foram criados os mesmos, exemplos de bases existentes são da CAIDA - Cooperative Association for Internet
Data Analysis, LBNL - Lawrence Berkeley National Laboratory e ICSI .

Buscando abordar o máximo de possibilidades e levando em consideração os problemas das bases de dados anteriores, o ISCX decidiu então formular um novo conjunto de dados que pudesse ajudar pesquisadores da área de IDS, tendo assim, acesso a um benchmark mais realista e abrangente, melhorando então a qualidade dos testes e estudos, estudos estes que atraem atenções devido ao grande volume de informações, e a possibilidade de se usufruir de grande parte delas.

Uma das maiores preocupações era tornar a DB o mais realista possível, por mais difícil que isso pareça, então os pesquisadores simularam o comportamento dos usuários através de uma “Central de Usuários”, captando os perfis dos mesmos, evitando assim características que não refletissem a realidade, o que poderia interferir no resultado final.

Para isso foram utilizadas 21 maquinas, todas elas com Windows, dividas em, Win XP – SP1, SP2 e SP3, e também Windows 7, totalizando 4 grupos de maquinas.

Em um dos passos seguidos para efetuar a invasão foi possível detectar informações do servidor principal, que possui o SO Ubuntu Server 10.04 com alguns serviços ativos, um servidor NAT também com Ubuntu e um segundo servidor com Windows server 2003 gerenciando serviços de Web.

Os ataques iniciaram na Sexta-feira 11 de Junho às 00:01:06 e durou exatamente 7 dias, terminando na Sexta-feira 18 de Junho.

A distribuição dos ataques foi a seguinte:

Sexta	Normal Activity. No malicious activity
Sabado	Normal Activity. No malicious activity
Domingo	Infiltrating the network from inside + Normal Activity
Segunda	HTTP Denial of Service + Normal Activity
Terça	Distributed Denial of Service using an IRC Botnet
Quarta	Normal Activity. No malicious activity
Quinta	Brute Force SSH + Normal Activity

Relatório sobre o artigo “Toward developing a systematic approach to generate benchmark datasets for intrusion detection”

Gustavo Barbosa Barreto

Durante a semana de segunda a sexta há um aumento substancial no fluxo pelo manha e lenta nas tardes, sendo o tráfego HTTP o mais abundante na DB.

O cenário de ataque é composto pelos seguintes passos:

1) Information gathering and reconnaissance (passive and active)
2) Vulnerability identification and scanning
3) Gaining access and compromising a system
4) Maintaining access and creating backdoors
5) Covering tracks

Foram usados 4 cenários de ataque, sendo eles:

- Cenário 1: Infiltrating the network from the inside
- Cenário 2: HTTP denial of service
- Cenário 3: Distributed denial of service using an IRC Botnet
- Cenário 4: brute force SSH.

Segundo os autores do artigo, ainda não existe uma base de dados ótima para que se efetuem testes e estudos, pois há muitas variáveis que interferem no resultado final do experimento, sendo muito difícil explorar todas elas.

Dúvidas e questões a discutir:

1- Teria como a gente incorporar no plano de trabalho o estudo dos tipos de ataques? Por exemplo como fazer um ataque SSH Brute Force, etc.

2- O Bruno disse que o arquivo XML tá no HD.

3- Ataques de negação de serviço e botnet, o que são?