Conjunto de dados de avaliação DDoS (CIC-DDoS2019)

O ataque distribuído de negação de serviço (DDoS) é uma ameaça à segurança da rede que visa esgotar as redes alvo com tráfego malicioso. Embora muitos métodos estatísticos tenham sido projetados para detecção de ataques DDoS, projetar um detector em tempo real com baixa sobrecarga computacional ainda é uma das principais preocupações. Por outro lado, a avaliação de novos algoritmos e técnicas de detecção depende fortemente da existência de conjuntos de dados bem concebidos.

Neste artigo, primeiro revisamos os conjuntos de dados existentes de forma abrangente e propomos uma nova taxonomia para ataques DDoS. Em segundo lugar, geramos um novo conjunto de dados, nomeadamente CICDDoS2019, que corrige todas as deficiências atuais. Em terceiro lugar, utilizando o conjunto de dados gerado, propomos uma nova abordagem de detecção e classificação de famílias baseada em um conjunto de características de fluxo de rede. Por fim, fornecemos os conjuntos de recursos mais importantes para detectar diferentes tipos de ataques DDoS com seus pesos correspondentes.

1. Introdução

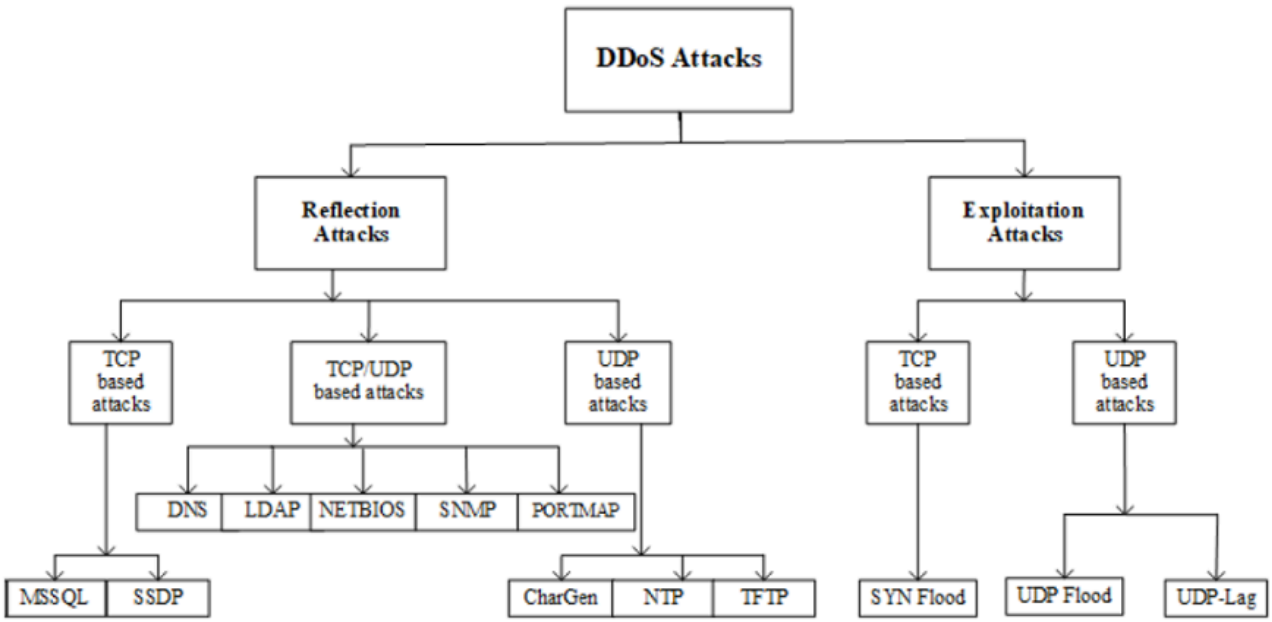
Existem vários estudos de pesquisa que propuseram taxonomias em relação aos ataques DDoS. Embora todos tenham feito um trabalho louvável ao propor novas taxonomias, o âmbito dos ataques tem sido até agora limitado. É necessário identificar novos ataques e criar novas taxonomias. Assim, analisamos novos ataques que podem ser realizados utilizando protocolos baseados em TCP/UDP na camada de aplicação e propusemos uma nova taxonomia. O restante desta subseção foi explicada a taxonomia detalhada dos ataques DDoS e ilustrada na Figura 1, em termos de ataques baseados em reflexão e ataques baseados em exploração.

DDoS baseado em reflexão: são aqueles tipos de ataques em que a identidade do invasor permanece oculta através da utilização de componentes legítimos de terceiros. Os pacotes são enviados para servidores refletores por invasores com endereço IP de origem definido para o endereço IP da vítima alvo para sobrecarregá-la com pacotes de resposta. Esses ataques podem ser realizados através de protocolos da camada de aplicação usando protocolos da camada de transporte, ou seja, protocolo de controle de transmissão (TCP), protocolo de datagrama de usuário (UDP) ou através de uma combinação de ambos. Como mostra a Figura 1, nesta categoria, os ataques baseados em TCP incluem MSSQL, SSDP, enquanto os ataques baseados em UDP incluem CharGen, NTP e TFTP. Existem certos ataques que podem ser realizados usando TCP ou UDP, como DNS, LDAP, NETBIOS e SNMP.

Ataques baseados em exploração: são aqueles tipos de ataques em que a identidade do invasor permanece oculta através da utilização de componentes legítimos de terceiros. Os pacotes são enviados para servidores refletores por invasores com o endereço IP de origem definido como o endereço IP da vítima alvo para sobrecarregar a vítima com pacotes de resposta. Esses ataques também podem ser realizados através de protocolos da camada de aplicação usando protocolos da camada de transporte, ou seja, TCP e UDP. Os ataques de

exploração baseados em TCP incluem inundação SYN e os ataques baseados em UDP incluem inundação UDP e UDP-Lag. O ataque de inundação UDP é iniciado no host remoto enviando um grande número de pacotes UDP.

Esses pacotes UDP são enviados para portas aleatórias na máquina de destino a uma taxa muito alta. Como resultado, a largura de banda disponível da rede se esgota, o sistema trava e o desempenho diminui. Por outro lado, a inundação SYN também consome recursos do servidor ao explorar o handshake TCP de três vias. Este ataque é iniciado enviando pacotes SYN repetidos para a máquina alvo até que o servidor trave/mau funcionamento. O ataque UDP-Lag é aquele tipo de ataque que interrompe a conexão entre o cliente e o servidor. Este ataque é usado principalmente em jogos online onde os jogadores desejam desacelerar/interromper o movimento de outros jogadores para superá-los. Esse ataque pode ser realizado de duas maneiras, ou seja, usando um switch de hardware conhecido como lag switch ou por um programa de software que roda na rede e consome a largura de banda de outros usuários.



2. Conjunto de dados

CICDDoS2019 contém ataques DDoS comuns benignos e mais atualizados, que se assemelham aos verdadeiros dados do mundo real (PCAPs). Também inclui os resultados da análise de tráfego de rede usando CICFlowMeter-V3 (//www.unb.ca/cic/research/applications.html#CICFlowMeter) com fluxos rotulados com base no carimbo de data/hora, IPs de origem e destino, portas de origem e destino, protocolos e ataque (arquivos CSV).

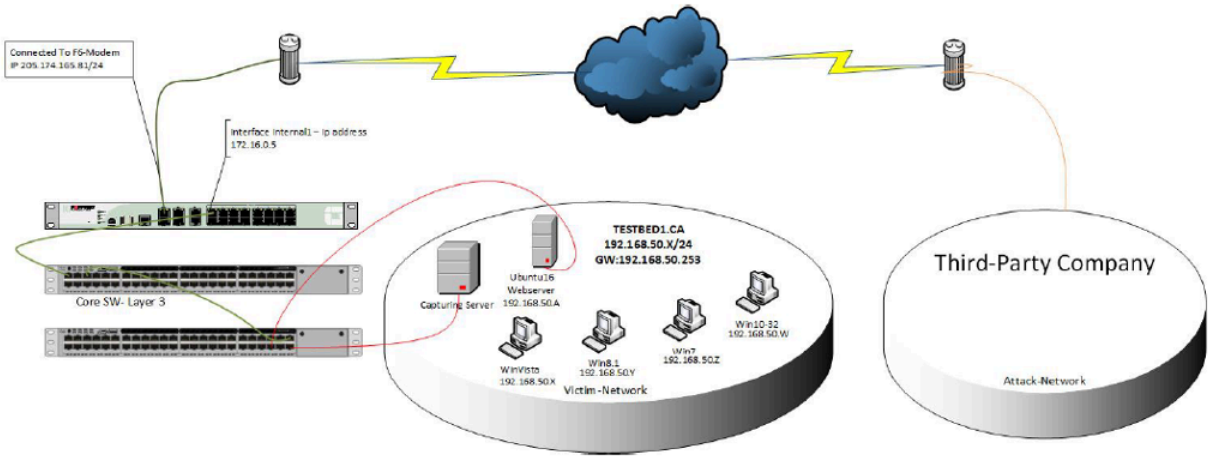


Figure 2: Testbed Architecture

A geração de tráfego de fundo realista foi nossa principal prioridade na construção deste conjunto de dados. Usamos nosso sistema B-Profile proposto (Sharafaldin, et al. 2016) para traçar o perfil do comportamento abstrato das interações humanas e gerar tráfego de fundo benigno naturalista no ambiente de teste proposto (Figura 2). Para este conjunto de dados, construímos o comportamento abstrato de 25 usuários com base nos protocolos HTTP, HTTPS, FTP, SSH e e-mail.

Máquina	SO	IPs
Servidor	Ubuntu 16.04 (servidor web)	192.168.50.1 (primeiro dia) 192.168.50.4 (segundo dia)

Máquina	SO	IPs
Firewall	Fortuna	205.174.165.81
PCs (primeiro dia)	Ganhe 7	192.168.50.8
	Win Vista	192.168.50.5
	Ganhe 8.1	192.168.50.6
	Ganhe 10	192.168.50.7
PCs (segundo dia)	Ganhe 7	192.168.50.9
	Win Vista	192.168.50.6
	Ganhe 8.1	192.168.50.7
	Ganhe 10	192.168.50.8

Neste conjunto de dados, temos diferentes ataques DDoS reflexivos modernos, como PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS e SNMP. Os ataques foram posteriormente executados durante este período. Como mostra a Tabela III, executamos 12 ataques DDoS incluindo NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN e TFTP no dia de treinamento e 7 ataques incluindo PortScan, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag e SYN no dia de testes. O volume de tráfego para WebDDoS foi muito baixo e o PortScan acabou de ser executado no dia de testes e será desconhecido para avaliação do modelo proposto.

Dias	Ataques	Tempo de ataque

Primeiro dia	Mapa de Porto	9:43 - 9:51
	NetBIOS	10h00 - 10h09
	LDAP	10h21 - 10h30
	MSSQL	10h33 - 10h42
	UDP	10h53 - 11h03
	Atraso UDP	11h14 - 11h24
	SIN	11h28 - 17h35
Segundo dia	NTP	10h35 - 10h45
	DNS	10h52 - 11h05
	LDAP	11h22 - 11h32
	MSSQL	11h36 - 11h45
	NetBIOS	11h50 - 12h00
	SNMP	12h12 - 12h23
	SSDP	12h27 - 12h37
	UDP	12h45 - 13h09
	Atraso UDP	13h11 - 13h15
	WebDDoS	13h18 - 13h29
	SIN	13:29 - 13:34
	TFTP	13h35 - 17h15

3. Usando o conjunto de dados

O conjunto de dados foi organizado por dia. Para cada dia, registramos os dados brutos, incluindo o tráfego de rede (Pcaps) e logs de eventos (logs de eventos do Windows e Ubuntu) por máquina. No processo de extração de recursos dos dados brutos, utilizamos o CICFlowMeter-V3 (//www.unb.ca/cic/research/applications.html#CICFlowMeter) e extraímos mais de 80 recursos de tráfego e os salvamos como um arquivo CSV por máquina.

Se quiser usar técnicas de IA para análise, você pode baixar nossos arquivos de dados gerados (CSV) e analisar o tráfego de rede.

Se quiser usar um novo extrator de recursos, você poderá usar os arquivos brutos capturados (PCAP) para extrair seus recursos. E então, você pode usar as técnicas de mineração de dados para analisar os dados gerados.

Exemplo de webinar de uso de conjunto de dados: " Aprimorando a generalização em sistemas de detecção de ataques DDoS por meio de abordagens de aprendizagem por transferência e aprendizagem por conjunto (https://youtu.be/zaRsIJy21xM) " pelo Dr. Mahdi Rabbani, pesquisador de pós-doutorado, Instituto Canadense de Segurança Cibernética e perguntas e respostas com o Dr.

4. Licença

Você pode redistribuir, republicar e espelhar o conjunto de dados CICDDoS2019 de qualquer forma. No entanto, qualquer uso ou redistribuição dos dados deve incluir uma citação ao conjunto de dados CICDDoS2019 e ao artigo publicado relacionado. Um artigo de pesquisa que descreve os detalhes da análise do conjunto de dados IDS/IPS semelhantes e princípios relacionados:

- Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak e Ali A. Ghorbani, " Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy (https://ieeexplore.ieee.org/abstract/document/8888419) ", IEEE 53ª Conferência Internacional Carnahan sobre Tecnologia de Segurança, Chennai, Índia, 2019.

Baixe este conjunto de dados >

(http://205.174.165.80/CICDataset/CICDDoS2019/)

Recursos

Sobre a UNB >

Mapas do campus >

Segurança do campus >

Carreiras na UNB >

Serviços na UNB >

Serviços de conferência >

Bibliotecas >

Educação on-line e contínua >

Liderança >

Conecte-se com a UNB

Entre em contato com a UNB (//www.unb.ca/contact/)

(https://www.facebook.com/uofnb)

(https://twitter.com/UNB)

(https://ca.linkedin.com/school/university-of-new-brunswick/)