1

Ataques (básicos) a uma rede local

João Fiuza de Alencastro 15/0131933

Abstract—Este relatório não tem um ataque principal em questão, aqui é onde comecamos a falar sobre ataques simples em geral, ataques conhecidos, como, por exemplo, Gathering, DoS, Flood, entre outros.

Index Terms—Ataques, redes, LAN, ARP, DDoS, Gathering, Flood, BruteForce, HTTP, IP, NMap, Python3.

I. Introduction

S ataques mencionados a cima são somente o primeiro passo para ataques maiores. Por esse motivo, ataques simples podem acabar se tornando extremamente perigosos.

Uma das principais solucões para ataques externos é a implementação de uma IDS (Invasion Detection System), uma aplicação, normalmente local, que monitora a rede ou os sistemas à procura de invasores ou softwares maliciosos.

Abaixo são apresentados alguns dos principais ataques que já foram muito bem sucedidos no passado e continuam sendo efetivos em sistemas mais vulneráveis.

A. NMap

Tema já abordado no relatório NMap[1], porém de extrema importância para o processo de 'information Gathering'. Também conhecido como Port Scanner, o NMap pode almejar de sistemas a redes inteiras e é já é utilizado por diversos frameworks conhecidos.

B. Flood

A proposta do *Flood*, como o nome já indica, é encher/"entupir" algo ou alguém com algo. Imaginemos uma analogia básica para fins didáticos, um atendente de bar, por exemplo, está trabalhando em uma noite especial e 100 pessoas tentam fazer pedidos simultaneamente para ele, sem dúvida alguma, ele não conseguirá lidar com toda essa demanda e talvez até desista da tarefa. Pois, esse é o princípio do *Flood*, enviar pedidos em larga escala em um curto período de tempo.

C. DoS (Denial of Service)

O ataque de negação de serviço utiliza-se do princípio do *Flood*, entupindo os recursos de um serviço com requisições, indisponibilizando aos usuários daquele serviço acesso e comunicação.

No experimento realizado, um simples script em python foi o suficiente para simular um pequeno ataque DoS ao serviço criado pelo colega próximo do laboratório, conectado à mesma LAN. O serviço era uma pequena aplicação HTTP na porta 8000 e o script cria 300 conexões HTTP.

Na imagem abaixo, pode ser visto que o IP da máquina localhost é 172.16.5.93 e foi feito um ataque DoS no endereço IP 172.16.5.91. Pode-se confirmar que o ataque foi bem

sucedido, pois a resposta HTTP é um código 200, indicando sucesso. O número na linha logo abaixo do código 200 há um número que se repete, 715, este número representa o número de bytes no diretório no qual a aplicação está diretamente associado.

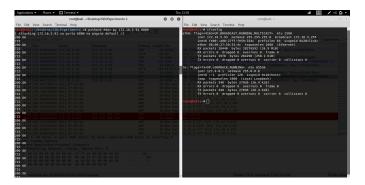


Fig. 1. Ataque DoS ao colega em mesma LAN

Na figura seguinte, podemos ver um mesmo ataque acontecendo, porém agora no próprio localhost, ou seja, em um serviço criado na mesma máquina atacante. Nessa imagem, é possível ver as requisições do lado do servidor, onde há informações do endereço IP do cliente, timestamp da requisição e o tipo da requisição, nesse caso o log do serviço é esse, porém pode ser muito diferente dependendo da aplicação. Perceba também, que o intervalo entre uma requisição e outra é tão pequena que todas na tela do terminal apresentam mesmo timestamp.

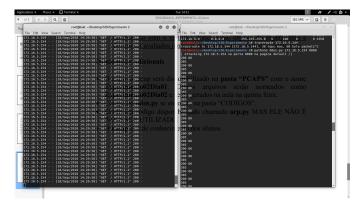


Fig. 2. Ataque DoS ao próprio endereço local

Ao analisar o tráfego da rede, fica claro como um ataque de negação de serviço acaba sendo muito custoso para conexões TCP, já que para requisição HTTP, até mesmo um simples 'GET', requer um 'three-way-handshake' da conexão segura fornecida pelo TCP. Na figura abaixo podemos ver um pequeno pedaço da análise do tráfego em modo promíscuo no WireShark no exato momento do ataque.

). Tim		Source	Destination	Protocol	Length Info	
		172.16.5.91	172,16,5,93	TOP	68 8880 - 52444 [ACK] Seq-1 Ack+71 Min+29055 Len-G T5val-2748374545 T5ecr+588879514	
		172.16.5.91	172.16.5.93	TOP	222 [TCP segment of a reassembled POU]	
		172.16.5.93	172.16.5.91	TOP	68 52444 - 8666 [ACK] Seq:71 Ack:155 Min:39336 Len:0 TSval=589879517 TSecr=2748374648	
		172.16.5.91	172.16.5.93	HITP	783 HTTP/1:0 200 DK (text/html)	
		172.16.5.93	172.16.5.91	TOP	68 52444 - 8000 [ACK] Seq-71 ACK-871 NIn-31744 Len-0 TSVal-588079517 TSecr-2740374648	
		172.16.5.93	172,16,5,91	TOP	88 52444 - 8800 [FIN. ACK] Seq=71 ACK=871 NLN=31744 Len=9 T9val=588979517 TSecr=2748974648	
		172.16.5.93	172.16.5.91	TOP	76 52446 - 8989 [SWI] Seg19 MINT29299 Lent9 MSS:1499 SACK PERM:1 TSwal:588079517 TSecr:0 VS:128	
		172.16.5.91	172,16,5,93	TOP	68 8000 - 52444 [ACK] Seq-071 Ack-72 Min-29055 Len-0 TSval-2740374849 TSecr-588079517	
		172.16.5.91	172,16,5,93	TOP	76 8880 - 52446 [SYN, ACK] Seq-0 ACK-1 NIN-29990 Len-0 MSS-1490 SACK_PERM-1 TS+k1-2740374649 TSecr-588079517 WS-128	
		172.16.5.93	172.16.5.91	TOP	69 52446 - 6660 [ACK] Seqri Ack:1 Nin:29012 Len:0 TSval:589079518 TSecr:2746074649	
		172.16.5.93	172.16.5.91	HITP	138 SET / HTTP/1.1	
		172.16.5.91	172.16.5.93	TOP	68 8880 - 52446 [ACK] Seq-1 Ack-71 Min-29056 Len-6 TSval-2748374650 TSecr-588079518	
		172.16.5.91	172.16.5.93	TOP	222 [TCP segment of a reassembled POU]	
		172.16.5.93	172.16.5.91	TOP	68 52446 - 6969 [ACK] Seq:71 Ack:155 Nin:39235 Len:0 TSvsl:588079520 TSecr:2740274652	
		172.16.5.91	172.16.5.93	HIID	783 HTTP/1.0 200 DK (text/html)	
		172.16.5.93	172.16.5.91	TOP	68 52446 - 8800 [ACK] Seq-71 ACK-871 NIn-31744 Len-8 TSVal-588879520 TSetr-2748374652	
		172.16.5.93	172.16.5.91	TOP	63 52446 - 8800 [FIN, MCK] Seq:71 Ack::871 NLN::31744 Len:8 T5xal::588879521 T5ecr::2748274652	
555 173	.355885891	172.16.5.93	172,16,5,91	TOP	76 52448 - 8000 [SYN] Seg-0 Min-29200 Len-0 MSS-1490 SACK PERM-1 TSwal-588079521 TSecr-0 WS-128	
		172.16.5.91	172.16.5.93	TOP	68 8860 - 52446 [ACK] Seq-871 Acx=72 MLn=29056 Len=0 TSVal=2748374853 TSecr=588079521	
		172.16.5.91	172.16.5.93	TOP	76 8880 - 52448 [SYNL MCM] Sequit Actual Natur-28990 Lenius MSS-1990 SADK_PERMIN TSWALH2748074653 TEecri-588079521 MS-128	
		172.16.5.93	172.16.5.91	TOP	68 52448 - 6660 [ACK] Segri Ackri Nimr29212 Lenni TSvalr588079522 TSecrr2748274653	
		172.16.5.93	172.16.5.91	HIID	138 GET / HTTP/1.1	
		172.16.5.91	172.16.5.93	TOP	68 8860 - 52448 [ACK] Seq-1 Ack-71 Min-29656 Len-8 TSval-2748374854 TSecr-588878522	
		172.16.5.91	172.16.5.93	TOP	222 [TCP segment of a reassembled POU]	
		172.16.5.93	172.16.5.91	TOP	68 52446 - 8000 [ACK] Seq-71 Ack-155 Nin-30335 Len-0 TSval-588079524 TSecr-2740374655	
563 173	.359201574	172.16.5.91	172.16.5.93	HTTP	783 HTTP/1:0 200 0K (text/html)	
		172.16.5.93	172.16.5.91	TOP	68 52448 - 6666 [ACK] Seq:71 ACk::871 NIn::31744 Len::0 TSval::589879524 TSecr::2748374656	
		172.16.5.93	172.16.5.91	TCP	68 52448 - 6000 [FIN, MCK] Segn71 Mckm871 Ninv21744 Lenn8 TSyalm588878524 TSecrn2748274656	
		172.16.5.93	172,16,5,91	TOP	76 52450 - 8000 [SYN] Seq-0 Min-29200 Len-0 MSS-1490 SACK_PERM-1 TSwal-588079525 TSecr-0 WS-128	
		172.16.5.91	172.16.5.93	TOP	68 8660 - 52442 [ACK] Seq-871 ACK-72 MIn-29656 Len-0 TSVsL-2748374656 TSetr-588879512	
568 173	.360003029	172.16.5.91	172.16.5.93	TOP	68 8960 - 52448 [ACK] Seq:871 Ack:72 Min:29856 Len:0 TSvx1:2748374857 TSecr:588078524	
		172.16.5.91	172.16.5.93	TOP	76 8880 - 52450 [578] ACK] Seq=0 Ack=1 Nin=28980 Len=0 MSS=1480 SACK_PERM=1 TSwal=2748374657 TSecr=588079605 MS=128	
		172.16.5.93	172.16.5.91	TOP	68 52450 - 8600 [ACK] Seq-1 Ack-1 Nin-29312 Len-0 T9val-589879525 TSetr-2748374657	
571 173	.369239289	172.16.5.93	172.16.5.91	HTTP	138 GET / HTTP/1.1	
		172.16.5.91	172.16.5.93	TOP	68 8000 - 52N50 [ACK] Seqri Ackv71 Ninv29055 LenvG T5val=2740374657 T5ecr=580070525	
		172.16.5.91	172.16.5.93	TOP	222 [TCP segment of a reassembled POU]	
		172.16.5.93	172.16.5.91	TOP	68 52450 - 8800 [ACK] Seq=71 Ack=155 MIn=38336 Len=0 TSvsl=588879528 TSecr=2748874658	
		172.16.5.91	172.16.5.93	HITP	783 HTTP/1:0 290 DK (text/html)	
		172.16.5.93	172.16.5.91	TOP	68 52450 - 8000 [ACK] Seq-71 Ack-871 Nin-31744 Len-0 TSval-588079528 TSecr-2748374659	
		172.16.5.93	172.16.5.91	TOP	88 52450 - 8800 [FIN. ACK] Seq-71 Ack-871 NLN-31744 Len-8 TSval-588079528 TSecr-2740374659	
		172.16.5.93	172.16.5.91	TOP	76 52452 - 6000 [SYN] Seq10 MIN129200 Len10 MSS:1490 SACK_PERM:1 TSval:588079528 TSecrib VS:128	
		172.16.5.91	172,16,5,93	TOP	68 8660 - 52450 [ACK] Seq-071 Ack+72 MIN-29055 Len-0 TSVs1+2740374600 TSecr=588079538	
		172,16,5,91	172,16,5,93		76 8880 - 52452 TSYN, ACKT 569-0 ACK-1 NIN-23990 Len-0 MSS-1490 SACK PERM-1 TS-k1-2740374661 TS-cr-588075528 MS-128	

Fig. 3. Pacotes ataque DoS

O DDoS continua sendo um ataque de negação de serviço da mesma forma, porém mais "inteligente", já que ele distribui a origem do ataque, fazendo com que várias máquinas diferentes façam algumas poucas requisições, totalizando em uma ataque generalizado e bem organizado. A maior vantagem do ataque ser distribuído dessa forma, é que o atacante gera uma dificuldade de localização grande, já que as requisições não são de um único endereço IP. Além disso, um ataque com várias máquinas dispõem de muito mais recursos do que somente uma máquina gerando requisições.

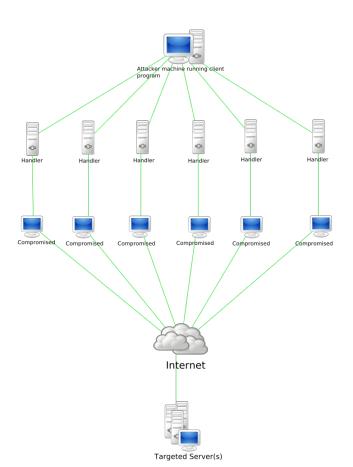


Fig. 4. Topologia clássica de um DDoS distribuído

II. CONCLUSION

APPENDIX A

PROOF OF THE FIRST ZONKLAR EQUATION

Appendix one text goes here.

APPENDIX B

Appendix two text goes here.

ACKNOWLEDGMENT REFERENCES

[1]

Michael Shell Biography text here.

PLACE PHOTO HERE

John Doe Biography text here.

Jane Doe Biography text here.