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.

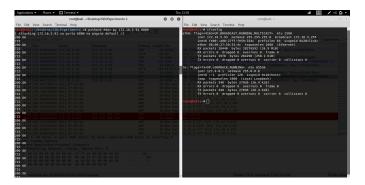


Fig. 1. Ataque DoS ao colega em mesma LAN

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.

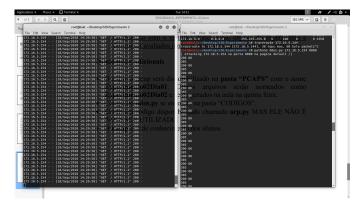


Fig. 2. Ataque DoS ao próprio endereço local

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.

Time	Source	Destination	Protocol	Length Info	-
530 173.3499294	58 172,16,5,91	172,16,5,93	TOP	68 8860 - 52444 FACKI Sep-1 Ack-71 Nin-29055 Len-6 T0xal-2748374545 TSecr-588878514	
539 173.3518270	60 172,16,5,91	172.16.5.93	TOP	222 [TCP segment of a reassembled POU]	
549 173.3518377	60 172.16.5.93	172.16.5.91	TOP	68 52444 - 8860 TACKI Sect71 Ack:155 Min:38336 Lens0 TSwalp588878517 TSecr:2748074648	
541 173.3518677	5 172.16.5.91	172.16.5.93	HTTP	783 HTTP/1.0 200 0K (text/bin1)	
542 173.3518725		172,16,5,91	TOP	89 52444 - 8880 [ACK] Deg-71 ACK-871 Min-31744 Len-8 TSyal-588879517 TSecr-2748374648	
643 173 3521611		172,16,5,91	TOP	89 52444 - 8980 [F]N, ACK Sequit Accust Ministral Lesie Tayali-589679527 Tayray248074648	_
544 173.3523357		172,16,5,91	TOP	76 52446 - 6600 [SNN] Secre Nurriscon Lerro Militago SACK PERMIT Taxalitago78517 Tierro VS-128	
545 173,3528695		172,16,5,93	TOP	61 8000 - 52444 FACKI Sec-071 Ack-72 Mir-2000 Leave TSyst-27-937-949 TSecr-55007537	_
846 173.3528942		172-16-5-93	TOP	76 8880 - 52446 [578] AKT SQUA AX11 NIN-2299 [401-8 833-1493 340X PRM-1 T542]-274074649 T5421-588079517 WS-128	
547 173 3524644		172,16,5,91	TO	65 SCARS - SCHOOL JOHN, MAJ SCHOOL ACKED MITHINGTO LANGE TO SCALES SCHOOL TO SCALE SCHOOL ACKED MITHINGTO LANGE TO SCALE SCHOOL ACKED ACKE	
540 173.3529454		172.16.5.91	HTTP	13 GET / HTP/1.1	
			TCP		
549 173.3538390		172.16.5.93	TOP	68 8860 - 52446 [ACK] Seq-1 ACK-71 NIn-29056 Len-8 TSval-2748374658 TSecr-588878518	
550 173.3553999				222 [TCP segment of a reassembled POU]	
551 173.3554077		172.16.5.91	TOP	68 52446 - 8000 [ACK] Seq=71 Ack=155 Win=30236 Len=0 TSval=580079520 TSecr=2740274652	
552 173.3554341		172.16.5.93	HILD	783 HTTP/1.0 200 GK (text/html)	
553 173.3554386		172.16.5.91	TOP	68 52446 - 8660 [ACK] Seq-71 ACK-871 MIn-31744 Len-0 TSval-589079520 TSecr-2740374652	
554 173.3557292		172.16.5.91	TOP	68 52446 - 6980 [FIN, ACK] Seg:71 Ack:871 NIn:31744 Les:8 TSval:588079521 TSecr:2746074652	=
555 173,3556650	91 172,16,5,93	172,16,5,91	TOP	76 52448 - 8000 (5YM) Secrit Minroscop Lerrit MSS-1490 SACK PERM-1 TSwal-588079521 TSecrit VS-128	
556 173.3566561	12 172.16.5.91	172,16,5,93	TOP	68 8880 - 52446 TACKI Sec-871 Ack-72 Min-29856 Len-8 TSval-2748374853 TSecr-588879521	
567 173 3566681	47 172 16 5 91	172,16,5,93	TOP	76 8660 - 52448 [SYN, ACK] Segui Ackul Ninu28900 Lenub MSSL1460 SACK PERMIT TSVALU2746374653 TSecri586079651 MS-128	-
558 171,1566658	16 172.16.5.93	172,16,5,91	TOP	68 SAME - 6000 PARK Secrit Acres Marchine Park Park Park Park Park Park Park Park	-
559 173.3567221	69 177 16 5 93	172,16,5,91	HTTD	138 SET / HTTP/1.1	
568 123 3526113		172,16,5,93	TOP	69 6960 - 52448 [ACK] Seq-1 ACK-71 MIn-20059 Len-0 TSval-2748374054 TSecr-588079522	
561 173.3591693		172.16.5.93	TOP	222 (TIP received of a requirement of a	
562 173.3591779		172,16,5,91	TOP	68 52440 - 8600 FACKI Sep-71 Ack-105 Min-30336 Len-0 TSyal-580079524 TSecr-2740374655	
563 173.3592015		172-16-5-93	HTTP	783 HTTP/1,0 200 0K (Lox//html)	
564 173,3592657		172,16,5,91	TOP	68 52448 - 8660 [ACK] Sequit Acku871 Minu31744 Lenu0 T9valu588079524 TSecru2740374656	
565 173.3594354		172,16,5,91	TOP	99 (CAMO * 0000 [KM] (ON) MANOYA MA	
566 173.3595994		172,16.5.91	TOP	08 52480 - 1800 [FIR, ANK] SEGVI AKKUIK MINISTAN LENNI STANDARTHEREVISE ISECTIONAL ISECTIONAL INC. 76 52450 - 2800 [SINI] SEGNO MINISTANDARTHEREVISE MASSILAND SACK PERMIT TSWAL-SERVISEZS TSECTION VS-128	
567 173 3516384		172,16,5,93	TOP	08 000 - SC442 (MX) Sep-071 ACK-72 MIN-20059 (min 75x) -27x457 TSer-7-8487952 (min 75x) -27x457 TSer-7-8487952	_
				89 8880 - 52442 [ACK] 569-871 ACK-72 MIN-29856 Len-8 19VAL-2748374856 15617-588079512	
568 173.3699839		172.16.5.93	TOP	68 8989 - 52448 [ACK] Seq:971 Ack:72 Min:29955 Len:9 T5vxl:2748274657 T5ecr:588078524	
569 173.3601542		172.16.5.93	TOP	76 8000 - 52450 [578] ACK] Seq=0 Ack=1 NLn=28900 Len=0 MSS=1460 SACK_PERN=1 TSval=2740374657 TSvcr=588075025 NS=120	
570 173.3601739		172.16.5.91	TOP	68 52450 - 8000 [ACK] Seq-1 Ack-1 NLn-29312 Len-0 T9val-589079525 T5etr-2740374657	
571 173.3692392		172.16.5.91	HTTP	138 GET / HTTP/1.1	
572 173.3605566		172.16.5.93	TOP	68 8880 - 52450 [ACK] Seq=1 Ack=71 Min=20055 Len=0 TSvsl=2748374657 TSec=588878525	
573 173.3826141		172.16.5.93	TOP	222 [TCP segment of a reassembled POU]	
574 173.3626273		172.16.5.91	TOP	68 52450 - 6660 [ACK] Seq=71 Ack=155 MIn=38330 Len=0 T9val=588079528 TSecr=2748074658	
575 173,3626583	58 172.16.5.91	172,16,5,93	HTTP	783 HTTP/1.0 250 (K. (text/html)	
576 173,3626635	45 172.16.5.93	172,16,5,91	TOP	98 52450 - 8000 FACKI Sep-71 ACK-071 Min-31744 Len-0 TSval-589079528 TSecr-2740374650	
577 273.3830215		172,16,5,91	TOP	85 52450 - 8000 [F]N. ACK Sco-71 ACK-871 NIN-31744 Len-8 TSval-959879528 TSecr-2748874659	-
578 173,3532968		172,16,5,91	TOP	76 52452 - 8880 [SYN] Segi0 Mini29200 Leni0 MSS:1480 SACK PERM:1 TSxx1:588079528 TSecr:0 WS:128	
579 173,3635627		172,16,5,93	TOP	61 650 - 5010 AN SWITS AND SWITS AND SWITS	_
580 273.3846746		172,16,5,93	TOP	76 8889 52452 (57N) ACKI SKIPS ACKI NIN-22990 (58N) 855-1498 35CC PERF-1 T5+21-274034861 T5+cr-588079528 95-128	_
	-				
2 esp 2 certo 20				Packets: 3754 : Displayed: 3754 (100.0%) - Load time: 00.29	Profile:

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 um 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.

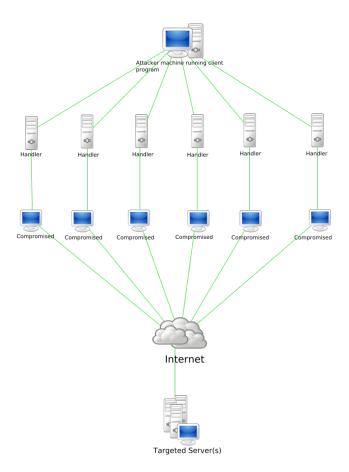


Fig. 4. Topologia clássica de um DDoS distribuído

II. CONCLUSION

Excluindo as descobertas de vulnerabilidades, ataques de *Flood* são, usualmente, custosos para o atacante também. Eles comprometem as conexões de um certo serviço, porém seus recursos ficam inutilizáveis. Por este motivo, hoje, atacantes utilizam-se de máquina alheias espalhadas pelo globo para realizar ataques distribuídos. E esse processo acontece, na maioria das vezes, sem o consentimento do dono da máquina, às vezes por ele baixar uma aplicação de fontes não confiáveis.

Ataques de negação de serviço podem ser prevenidos por utilização de IDS (Invasion Detection System) em sua rede ou sistema. É necessário que haja algum processo específico para a detecção de intrusos ou atividades suspeitas, o caso do DoS. Ele pode ser o responsável por "perceber" múltiplas requisições, enviadas em um tempo realizável somente por máquinas, e deve ser capaz de "negar" o serviço demandado, e assim surge o nome do ataque.

REFERENCES

- [1] https://en.wikipedia.org/wiki/Intrusion-detection-system
- [2] https://pt.wikipedia.org/wiki/Ataque-de-negacao-de-servico