Instituto de Informática (INF)
Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre - RS
URL: https://www.inf.ufrgs.br

Orientador: Prof. Dr. Lisandro Zambenedetti Granville
Coorientador: Leandro Bertholdo
Grupo de Redes de Computadores
E-mail: granville@inf.ufrgs.br
leandro.bertholdo@ufrgs.br

AnyPot - Honeypot Anycast

1 Introdução e Motivação

Um **Honeypot** [5] é um recurso de segurança projetado para ser um alvo atrativo para invasores. Seu propósito é detectar, monitorar e analisar atividades maliciosas. Honeypots são um sucesso como sistema de defesa de segurança cibernética se tornando espiões em botnets, expondo sua infraestrutura.

Anycast [4] é uma técnica de comunicação de rede na qual vários dispositivos são configurados com o mesmo endereço IP, permitindo que o tráfego seja direcionado automaticamente para o dispositivo mais próximo ou disponível na rede através do controle granular do roteamento.

Moving Target [3] é uma abordagem promissora para defesa que tenta reequilibrar o cenário cibernético. Ela altera a natureza estática dos sistemas da internet permitindo que uma aplicação possa migrar sua localização geografica aumentando o tempo e esforço para os atacantes.

Um honeypot anycast permite a honeypots incorporar a ideia de moving target através do controle do catchment anycast. Catchment refere-se ao que site irá receber o trafego de determinada rede de origem. O mapeamento de catchment anycast permite descobrir endereços falsificados (IP Spoofing) atacando um determinado serviço. Aplicando-se a tecnica anycast associada a honeypots nos permite identificar ataques originados em IPs forjados, uma informação importante para descobrir a origem de ataques DDoS de reflexão.

O projeto tem várias fases que os alunos pode abordar (diferentes TCCs) em discussão com os orientadores:

1- O primeiro passo é configurar uma rede anycast capaz de mapear o abrangência do endereço IPv4 quais redes escolhem enviar tráfego para Amsterdam em vez de Seattle ou São Paulo (Tangled [1] e Peering [6])

2- Empacotar um honeypot multiprotocolo [2] em docker (ou outro) e distribuí-lo em todos os sites anycast.

3- Utilizar datasets de tabelas de rotas e traceroutes para construir uma arvore de AS-paths a partir de nodos anycast.

4- Analisar as fontes IP de atacantes contra o mapeamento anycast e identificar regiões mundiais que geram mais tráfego falsificado.

5- Reconfigurar o roteamento anycast e observar novamente a abrangência para chegar mais perto do sistema autônomo que originou essas solicitações.

2 Descrição das Atividades

As atividades a serem desenvolvidas durante o TG1 e TG2 são descritas abaixo:

A1. **Estudo sobre redes Anycast:** Familiarizar-se com conceitos como redes anycast, anycast catchment, e active probing.

A2. **Estudo sobre Honeypots:** O aluno deve se familiarizar com as informações que podem ser obtidas utilizando diversos tipos de honeypots e tecnicas utilizadas para cruzar essas informações.

A3. **Revisão bibliográfica:** Revisão bibliografica sobre anycast, catchment control, e técnicas utilizadas em honeypots.

A4. **Definição e delimitação de escopo da proposta:** Esta etapa compreende a definição dos requisitos e objetivos que deverão ser atingidos. O trabalho deve considerar pesquisas recentes e a inovação da abordagem incorporando anycast a honeypots.

A5. **Design da Solução:** A solução deve ser projetada de forma flexível e genérica (ex. utilizando uma solução em docker para honeypots) para ser implementada em uma rede anycast como Tangled ou Peering. A implementação será usada para demonstrar que a solução atende aos requisitos e objetivos pretendidos (ex. quantificar trafego com origem forjada).

A6. **Avaliação de resultados:** A solução proposta deve ser comparada com soluções existentes e inovação proposta.

A7. **Escrita do TCC:** Essa atividade é continua e deverá ser realizada ao longo de todo o trabalho conforme discussao com os orientadores.

As atividades deverão ser realizadas ao longo de 1 ano durante as cadeiras de Trabalho de Graduação (TG) 1 e 2. As atividades de escrita deverão ocorrer em paralelo com o desenvolvimento prático do trabalho. Sugere-se que os seguintes capítulos estejam concluídos ao final de cada uma das cadeiras:

- **TG1**: Introdução e Motivação, Referencial Teórico e Trabalhos Relacionados;
- **TG2**: Abordagem, Implementações, Avaliações e Conclusões.

Porém, tais atividades e entregas poderão ser alteradas se acordadas com os orientadores para um melhor desenvolvimento do trabalho e adequação a metas/resultados do trabalho.

3 Requisitos

- Conceitos básicos de cibersegurança e honeypots;
- Interesse por redes de computadores e medições na Internet;
- Cursado as disciplinas de:
  - Redes de Computadores 1 e 2;

References

[1] L. M. Bertholdo, J. M. Ceron, W. B. Vries, R. D. O. Schmidt, L. Z. Granville, R. V. Rijswijk-Deij, and A. Pras, "TANGLED: A Cooperative Anycast Testbed," Proceedings of the IM 2021 - 2021 IFIP/IEEE International Symposium on Integrated Network Management, May 2021, pp. 766–771.

[2] T. Heinrich, R. R. Obelheiro, and C. A. Maziero, "New kids on the drdos block: Characterizing multiprotocol and carpet bombing attacks," Passive and Active Measurement: 22nd International Conference, PAM 2021, Virtual Event, March 29–April 1, 2021, Proceedings 22. Springer, 2021, pp. 269–283.

[3] Q. Jia, H. Wang, D. Fleck, F. Li, A. Stavrou, and W. Powell, "Catch me if you can: A cloud-enabled ddos defense," Proceedings of the International Conference on Dependable Systems and Networks. IEEE, 2014, pp. 264–275.

[4] T. Koch, E. Katz-Bassett, J. Heidemann, M. Calder, C. Ardi, and K. Li, "Anycast in context: A tale of two systems," Proceedings of the 2021 ACM SIGCOMM 2021 Conference, ser. SIGCOMM '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 398–417. [Online]. Available: https://doi.org/10.1145/3452296.3472891

[5] A. Mairh, D. Barik, K. Verma, and D. Jena, "Honeypot in network security: a survey," Proceedings of the 2011 international conference on communication, computing & security, 2011, pp. 600–605.

[6] B. Schlinker, K. Zarifis, I. Cunha, N. Feamster, and E. Katz-Bassett, "PEERING: An AS for Us," Proceedings of the 13th ACM Workshop on Hot Topics in Networks, ser. HotNets-XIII. New York, NY, USA: Association for Computing Machinery, 2014, pp. 1–7. [Online]. Available: https://doi.org/10.1145/2670518.2673887