Avaliação e comparação de Honeypots

Fabiano da Silva Santos[1], Roben Castagna Lunardi[1*]
Orientador(a)[*]
[1]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS) - Campus Restinga. Porto Alegre, RS

Honeypots são sistemas utilizados em redes de computadores para atrair e desviar a atenção de invasores. Estes sistemas são como "iscas" em uma rede para atrair ciberataques. Ao utilizá-los em uma rede, as equipes de segurança se tornam capazes de observar e analisar, estudando as tentativas de hacking e vulnerabilidades em seus sistemas. A partir disso, reforçar suas políticas de segurança e adotar práticas preventivas mais eficazes. Cada um desses sistemas possui suas propriedades de funcionamento específicas, tais como: tentativas de autenticação, captura de malwares, captura de spam até emulação de sistemas operacionais completos. O objetivo deste trabalho é comparar estes sistemas no intuito de auxiliar equipes de cibersegurança na adoção de acordo com sua demanda. Para fazer esta comparação, foi utilizada a ferramenta T-pot, que simula uma honeynet com diversos honeypots para os mais diversos serviços, protocolos e sistemas operacionais. Esta ferramenta foi utilizada em um sistema Linux Ubuntu Server 24.04 virtualizado em um servidor Proxmox. Para executar os testes foi utilizado o Kali Linux que possui ferramentas para PENTEST, como Metasploit, John the Ripper, e também ferramentas para varreduras como o Nmap. Dentre as muitas opções, são abordados os sistemas Cowrie, Dionaea e Mailoney. O Cowrie simula serviços SSH e Telnet. Os logs desse sistema possuem detalhes, como tentativas de autenticação, IP de origem e tentativas de força bruta, e também interações via shell, para análise posterior. Isso torna possível a reconstrução completa da sessão. Por sua vez, o Dionaea emula diversos serviços vulneráveis (como SMB, HTTP, MYSQL, etc.), capturando exploits, maliciosos. Além disso, esse sistema é capaz também de protocolar a porta alvo, IP de origem e a porta de destino. Por sua vez, o Mailoney foca no protocolo SMTP, registrando IPs, portas e credenciais de autenticação. A metodologia de teste seguiu-se dessa forma: O Nmap para varreduras e descoberta de serviços, enquanto o Metasploit para exploração de vulnerabilidades e acesso pós-invasão. Por fim, identificamos que o Cowrie se mostrou o melhor sistema na captura de interações SSH, permitindo reconstruir sessões. O Dionaea é eficaz na identificação de exploits e payloads maliciosos em muitos serviços. Da mesma forma, o Mailoney se mostra eficaz na coleta de dados e atividades SMTP, como credenciais e tentativas de autenticação. Portanto, conclui-se que, a escolha de um honeypot varia de acordo com o ambiente e a necessidade da organização onde ele será empregado. A escolha de um honeypot de forma errada pode comprometer o ambiente e a análise de ameaças. Porém, a escolha correta amplia a capacidade de detecção e torna ainda melhor a implementação de boas práticas de segurança.

Palavras-chave: Honeypots; PENTEST ; Logs.