Análise e Desenvolvimento de Sistemas – Segurança da Informação - Avaliação P1

Nome: Gustavo Teles Bonifácio Data: 17/12/2020

1. **Qual a função da ferramenta snort? Em quais situações ela deve ser utilizada?**
   A ferramenta Snort é uma ferramenta de "Defesa". Já que através de linhas de código e um pouco de conhecimentos em protocolos, é possível saber tudo que se passa não só no sistema, mas na rede. Já que da para analisar os tráfegos e registrar pacotes.
2. **Um scan de portas TCP utiliza as flags para determinar se uma porta está aberta ou não. Como um scan UDP consegue determinar se a porta está aberta ou não já que não possui tais flags?**
   Através da ausência de resposta no pacote, já que quando a porta esta fechada, o sistema responde como se estivesse inacessível.
4. **Uma máquina com o SO windows chega para você e é preciso quebrar a senha de uma conta local. Quais passos/ferramentas você faria/utilizaria? (não é necessário detalhar os comandos e sim os passos gerais!)**
   Por ser mais rápido e ágil, possivelmente usaria a redefinição/deletando a senha, utilizando a ferramenta no Kali Linux onde é possível manipular o arquivo SAM do Windows.
5. **No crack de senhas, existem vários tipos de ataques, como por exemplo: lista de dicionário, força bruta e sniffer (entre outros). Explique, com suas palavras, como cada um destes ataques funcionam bem como sua eficiência em quebrar uma senha (ferramentas utilizadas, se precisa ou não acesso a máquina, tempo, etc).**
   Alguns ataques implicados nessa questão, são na maioria, dependentes do Hardware em questão. E isso pode haver mudanças na velocidade de descobrimentos de senha, e um pouquinho de sorte.
   Os ataques de dicionário se usam um world list (lista de palavras em português, ou simplesmente dicionário), para se quebrar uma senha. O tempo de quebra de senha nesse ataque, varia muito, já que dependendo da ferramenta, é possível utilizar vários "caminhos" opcionais, exemplo: duplicação de palavras, utilização de letras maiúsculas, números etc. Assim tornando o tempo maior ou menor, entretanto, é quase nula as chances de obter a senha dessa forma. Já que tudo depende da lista de palavras.
   O ataque de sniffer é possível através da rede. Onde uma pessoa que acessa um determinado site sem uma criptografia esperada, é possível capturar as senhas, e todos os outros tipos de dados que uma pessoa costumeiramente colocaria num formulário de registro e/ou login.
   O ataque de força bruta utiliza um método de tentativa e erro, entretanto, esse pode ser o mais demorado de todos, já que ele não utiliza uma lista predeterminada e ainda mais, pode demorar ainda mais já que é possível obter outros "passos opcionais" numa string. Nesse ataque, a única coisa que podemos predeterminar, é os caracteres que se pode ter e a quantidade que imaginamos ser. Por exemplo: temos "ABC", e quantidade de 2, então começa; AA, aa, Aa, aA, Ab, aB, ab e etc.
6. **Os elementos da segurança da informação incluem confidencialidade, integridade e disponibilidade. Qual técnica abaixo está relacionada com integridade?** c. hash
7. **Baseando-se na figura abaixo, qual comando nmap para fazer: a. um ping UDP o mais silencioso possível?** -sP -PU -t0

b. um scan com o 3 way handshake incompleto, sem utilização do protocolo ICMP e o mais rápido possível? -sX

8. **Um analista de segurança está confuso com um incidente recente. Um hacker obteve acesso a sua máquina e roubou dados da empresa. Um scan completo foi realizado na máquina e nada foi encontrado. Qual(is) das alternativas melhor descreve o ocorrido?**
   a. O hacker tirou vantagem de uma vulnerabilidade zero-day na máquina
9. **Um hacker fará um scan em uma determinada máquina. Ele deseja se passar por outro IP. Qual técnica de scan o hacker deverá utilizar?** e. scan idle
10. **O hacker deseja quebrar uma senha qualquer e tentará algumas combinações possíveis de caracteres e alterando alguns destes por outros, por exemplo: uma palavra com o caractere "a" será testado com "a" e com "@". Qual(is) técnica(s) ele está utilizando?** a. ataque híbrido