1.Introdução a ferramentas de Segurança da Informação

Para explorar uma vulnerabilidade, um agente de ameaça deve ter uma técnica ou ferramenta. O hacking ético envolve o uso de muitos tipos diferentes de ferramentas para testar a rede e os dispositivos finais. Atores de ameaças também criam várias ferramentas de hacking. Essas ferramentas são escritas explicitamente por motivos nefastos.

1.1 Crackers de senhas

As ferramentas de quebra de senha são frequentemente chamadas de ferramentas de recuperação de senha e podem ser usadas para quebrar ou recuperar a senha. Isso é feito removendo a senha original, depois de ignorar a criptografia de dados, ou pela descoberta direta da senha. Os crackers de senhas repetidamente fazem suposições para decifrar a senha e acessar o sistema. Exemplos destas ferramentas são John the Ripper, L0phtCrack, Hydra, Medusa e RainbowCrack.

1.2 Ferramentas de hacking sem fio

As redes sem fio são mais suscetíveis a ameaças à segurança da rede. As ferramentas de hackers sem fio são usadas para invadir intencionalmente uma rede sem fio para detectar vulnerabilidades de segurança. Exemplos de ferramentas são Aircrack-ng, KisMAC e NetStumbler.

1.3 Digitalização de rede e ferramentas de hacking

As ferramentas de verificação de rede são usadas para investigar dispositivos, servidores e hosts de rede em busca de portas TCP ou UDP abertas. Exemplos de ferramentas de digitalização incluem Nmap, NetScanTools, SuperScan e outros.

1.4 Ferramentas de elaboração de pacotes

Ferramentas de criação de pacotes são usadas para sondar e testar a robustez de um firewall usando pacotes forjados especialmente criados. Ferramentas deste tipo são Socar, Netcat, Nping e Nemesis.

1.5 Sniffers de pacotes

As ferramentas de sniffers de pacotes são usadas para capturar e analisar pacotes em LANs Ethernet ou WLANs tradicionais. Ferrasmentas deste tipo incluem Wireshark, Tcpdump, EtherApe, Fiddler, Ratproxy e SSLstrip.

1.6 Detectores de rootkit

Um detector de rootkit é um verificador de integridade de diretórios e arquivos usados por white hats. Exemplos de ferramentas são AIDE, Netfilter e PF: OpenBSD Packet Filter.

1.7 Fuzzers para pesquisar vulnerabilidades

São ferramentas usadas por agentes de ameaças ao tentar descobrir vulnerabilidades de segurança de um sistema de computador. Exemplos de difusores incluem Skipfish, Wapiti e W3af.

1.8 Ferramentas forense

Ferramentas forense são usadas para farejar qualquer vestígio de evidência existente em um sistema de computador específico. Exemplos de ferramentas incluem Sleuth Kit, Helix, Maltego e Encase.

1.9 Depuradores

Ferramentas de depuração são usadas para fazer engenharia reversa de arquivos binários ao escrever exploits. Eles também são usados por white hats ao analisar malware. As ferramentas de depuração incluem GBD, WinDbg, IDA pro e Immunity Debugger.

1.10 Ferramentas de criptografia

Estas ferramentas salvaguardam o conteúdo dos dados de uma organização quando são armazenados ou transmitidos. As ferramentas de criptografia usam esquemas de algoritmo para codificar os dados e evitar o acesso não autorizado aos dados. Exemplos são VeraCrypt, CipherShed, Open SSH, OpenVPN e Stunnel.

1.11 Ferramentas de exploração de vulnerabilidades

Essas ferramentas identificam se um host remoto é vulnerável a um ataque de segurança. Exemplos de ferramentas de exploração de vulnerabilidade incluem Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit e Netsparker.

1.12 Scanners de vulnerabilidades

Essas ferramentas examinam uma rede ou sistema para identificar portas abertas, além de também serem usadas para verificar vulnerabilidades conhecidas e verificar VMs, dispositivos BYOD e bancos de dados do cliente. Exemplos são Nipper, Securia, PSI, Core Impact, Nessus, SAINT e Open VAS.

1.13 Sistemas operacionais

Os sistemas operacionais de hacking são especialmente projetados, pré-carregados com ferramentas e tecnologias otimizadas para hackers. Exemplos de sistemas operacionais de hacking especialmente projetados incluem Kali Linux, SELinux, Knoppix, Parrot OS e BackBox Linux.