ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL DEPUTADO ROBERTO MESQUITA

CLARISSA VITÓRIA RODRIGUES SIQUEIRA
EVELLYN CLEYCIANE SOUSA LIMA

EVERSON SOUSA

SEGURANÇA DA INFORMAÇÃO

NMAP (NETWORK MAPPER)

GENERAL SAMPAIO-CEARÁ
2024

INTRODUÇÃO

O Nmap, ou Network Mapper, é uma das ferramentas mais poderosas e amplamente utilizadas para varredura de redes e auditoria de segurança. Ele foi desenvolvido por Gordon Lyon (também conhecido como Fyodor) e é uma ferramenta de código aberto disponível para várias plataformas, incluindo Windows, Linux e macOS. O Nmap é utilizado por administradores de rede, profissionais de segurança e hackers éticos para mapear redes, identificar hosts ativos, descobrir portas abertas e serviços em execução, e até mesmo detectar vulnerabilidades.

DESENVOLVIMENTO

Desde seu lançamento inicial em 1997, o Nmap passou por várias atualizações e melhorias. O desenvolvimento contínuo e a comunidade ativa de usuários contribuíram para tornar o Nmap uma ferramenta robusta e versátil. Aqui estão alguns dos recursos e funcionalidades mais importantes do Nmap:

Varredura de Hosts e Portas:
O Nmap pode identificar dispositivos ativos em uma rede e verificar quais portas estão abertas. Isso é fundamental para mapear a topologia de uma rede e descobrir possíveis pontos de entrada.

Detecção de Serviços e Versões:
Uma das funcionalidades mais poderosas do Nmap é sua capacidade de identificar serviços em execução e suas versões. Isso ajuda os profissionais de segurança a encontrar serviços desatualizados ou vulneráveis.

Scripting Engine (NSE):
O Nmap possui um mecanismo de scripts que permite a execução de scripts escritos em Lua para realizar tarefas específicas, como detectar vulnerabilidades ou realizar auditorias de segurança.

CONCLUSÃO

Hackers Éticos:

(White Hat) São profissionais de segurança que utilizam suas habilidades para proteger sistemas e redes. Eles realizam testes de penetração e auditorias de segurança para identificar e corrigir vulnerabilidades antes que hackers mal-intencionados possam explorá-las.

Eles ajudam a fortalecer a segurança cibernética, educar organizações sobre melhores práticas e proteger informações sensíveis contra acessos não autorizados.

REFERÊNCIA:

COPILOT: https://copilot.microsoft.com.