Relatório de Segurança

Escopo:

Certifique-se de que suas atividades permaneçam dentro do escopo do programa. Por exemplo, painéis de administração para serviços de data center que utilizamos estão fora do escopo porque não são de propriedade, hospedados e operados

Data em que foram feitos os testes 29/11/2022

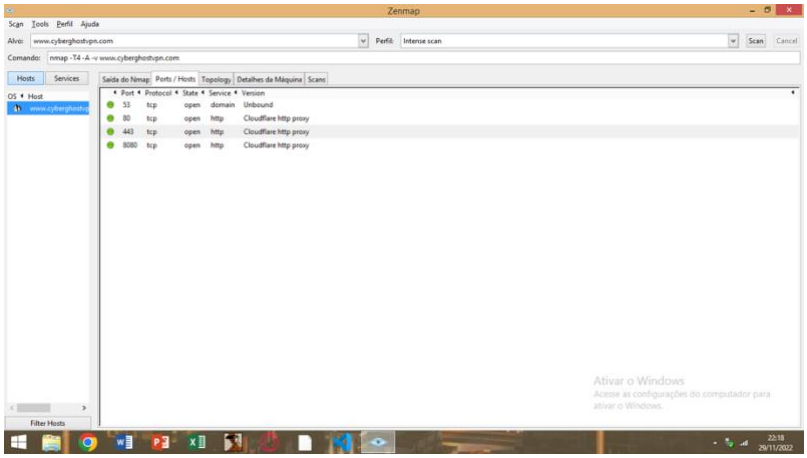
Empresa: Cyberghost

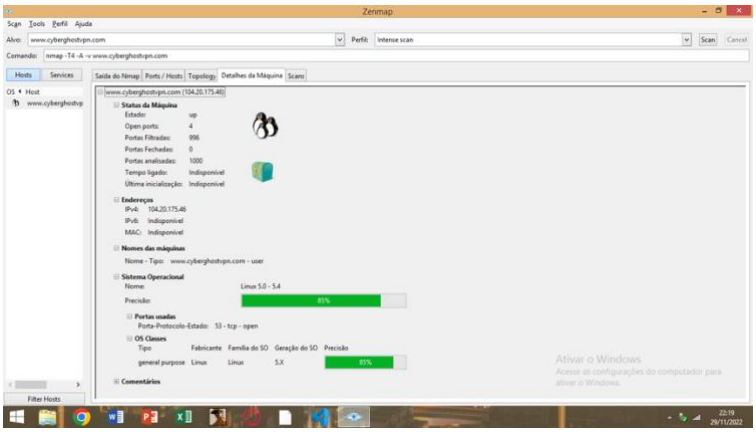
Fundada em 2011 em Bucareste, na Romênia, a CyberGhost é a criadora de uma das soluções de privacidade e segurança mais confiáveis do mundo. A empresa assegura e anonimiza a presença de usuários on-line de mais de 38 milhões usuários nos quatro cantos do mundo. A CyberGhost defende a privacidade como um direito básico do ser humano, tendo sido a primeira empresa do setor a publicar um relatório de transparência, ao mesmo tempo desenvolvendo novas tecnologias de criptografia orientada ao usuário para o futuro.

Subdomínios da Empresa:

Hospedeiro	Subdomínio	IP	ASN
cyberghostvpn.com	paris-s13-n01.cyberghostvpn.com		
cyberghostvpn.com	links.cyberghostvpn.com		
cyberghostvpn.com	lbfeed-prometheus2.cyberghostvpn.com		
cyberghostvpn.com	erfurt-s06-i01.cyberghostvpn.com		
cyberghostvpn.com	master.cyberghostvpn.com		
cyberghostvpn.com	zurich-s03-n01.cyberghostvpn.com		
cyberghostvpn.com	webadmin.cyberghostvpn.com		
cyberghostvpn.com	w.cyberghostvpn.com		
cyberghostvpn.com	security.cyberghostvpn.com		
cyberghostvpn.com	dev-api.cyberghostvpn.com		
cyberghostvpn.com	monitor.cyberghostvpn.com		
cyberghostvpn.com	db1.cyberghostvpn.com		

Portas e Sistemas operacionais do Site:





Software Usados no Site:

Executando wappalyzer em https://www.cyberghostvpn.com/pt_BR/

	Nome	Versão	Local na rede Internet	Categoria
	hCaptcha	1	https://www.hcaptcha.com	Segurança
	Sectigo	Nenhum	https://sectigo.com/	Autoridades certificadoras SSL/TLS
	Cloudflare	Nenhum	http://www.cloudflare.com	CDN
	HTTP/3	Nenhum	https://httpwg.org/	Diversos

Ips Ativos no Site:

104.20.174.46
142.250.219.4
105.16.174.4
172.217.29.14

Firewall que a Empresa usa:

Hospedeiro	IP	WAF Detectado
www.cyberghostvpn.com	104.20.174.46	Cloudflare

Vulnerabilidades de engenharia social:

Restaurantes e Bares próximos:

Taco grill End: (1800 Marketview Dr, Yorkville, IL 60560, Estados Unidos)

Wendy End: (1855 Marketview Dr, Yorkville, IL 60560, Estados Unidos)

Burg king End: (1835 Marketview Dr, Yorkville, IL 60560, Estados Unidos)

E-mails que já foram expostos:

Copyright@cyberghost.ro
(Jurídico)
Webmaster@cyberghost.ro
(Ti/engenharia)
Sales@cyberghost.ro
(Vendas)

Possível vulnerabilidade:

Os ips testados não apresentam nenhuma vulnerabilidade de nível grande ou médio, mas pode estar vulnerável a ataques de Dos e DDoS (Negação de serviço) um vulnerabilidade de nível Baixo.

Em um ataque de DDoS (negação de serviço distribuída), um invasor sobrecarrega seu alvo com tráfego de Internet indesejado para que o tráfego normal não atinja o destino pretendido

Sugestões para o Contratante:.

Para a possível Vulnerabilidade é aconselhável usar o software Blackhole

O roteamento Blackhole é uma estratégia que reduz o impacto de ataques DDoS. Consiste em redirecionar as solicitações para um endereço IP inválido. Essa medida mantém indisponível o IP alvo dos pacotes maliciosos. Nesse caso, não há diferenciação entre solicitações de acesso legítimas e maliciosas.

Sobre segurança nos e-mails da empresa:
Ter senhas fortes não colocar dados pessoais nas senhas
Utilizar carácteres randômicos para sua senha
Mistures números e carácteres especiais

Sobre Riscos de engenharia social:
Mantenha o anti vírus da empresa atualizado isto pode evitar o malware que vem através dos e-mails de phishing seja instalado automaticamente use um pacote como Kaspersky Antivírus para manter a sua rede de dados seguras
Configurar todas os e-mails da empresa com segurança de dois fatores é essencial para ter uma conta segura

Risco de funcionários com crachás em bares ou restaurantes é bem frequente
Aconselhável ter uma política de segurança para que não seja levado os crachás ou qualquer forma de informação que possa comprometer a empresa.

Software Usados durante o Teste:

Wappalyzer(mostra com o que o site são construídos qual cms o site usa)
Nmap
Detecto Waf (detecção de firewall do site)
Cmseek (detecção de cms)
Haveibeenpwned (verificar se os e-mail foram expostos)
Hunter oi (detecção dos e-mails da empresa)

Autorização e termo de pagamento

Autorização de Pentest
Eu, Cyberghost, autorizo Davi Santiago da Silva à conduzir atividades de verificação de segurança das seguintes aplicações e sistemas descritos abaixo.
· www.Cyberghostvpn.com, todos aplicações da página;
· Servidor de e-mail; hospedado pelo Hostgator;
· DNS, protegido Cloudflare;
· Tela de login;
As seguintes restrições se aplicam:
Autorização terá efeito de 29/11/2022 à 01/12/2022;
Proibido tentar ter acesso a datacenter que não estão hospedados e operados
Em conformidade com a concessão desta autorização, o Cliente declara que:
· O cliente tem um backup de todos os sistemas a serem testados e verificou que o backup está disponível para restauração ao estado antes do teste.
· O serviço envolve uso de ferramentas e técnicas desenvolvidas para detectar falhas de segurança, e que é impossível de identificar e eliminar todos os riscos envolvidos.
O pagamento será feito se for achado alguma falha ou vulnerabilidade de nível médio ou grave
Cachoeira BA, 29/11/2022

Assinatura: _____