Segurança da Informação

Prevenção de Ataques e Defesas
Soluções rápidas para contramedidas de ataques

Prof. Fábio Henrique Ribeiro Machado
fabiohenriquerm@gmail.com
Github.com/fabiohenriquerm/proxy

Contramedidas

PROBLEMAS	SOLUÇÕES
Varredura de endereços IP	Bloquear ICMP de entrada
Varredura de Portas	- IPS (Sistema de prevenção de intrusos). - Uso de serviços com Port knocking - Bloqueio no firewall
FootPrinting e FingerPrint (Enumeração)	- IPS e/ou Honeypot - Atualizar o arquivo robots.txt - Verificar os dados expostos no Whois - Hardening das permissões de arquivos, diretórios e usuários
Falhas de Software	- Atualizações - Serviços rodando como Usuários sem privilégios
Força-Bruta	- Bloqueio de conta após 3 erros - Bloqueio do IP no Firewall - Política rígida de senhas (mínimo 10 caracteres)
Redirecionamento de Tráfego (ARP Poisoning)	- Switch com ARP Inspection - ARP estático para o gateway nas máquinas - ArpON instalado nas máquinas
SNIFFER (Farejamento)	- Evitar o redirecionamento de tráfego - Criptografar os dados

Contramedidas

MITM Remoto	- Verificar certificado do site - Verificar se o proxy está ativado e remover se necessário
MITM Local	- Verificar Certificado - Impedir redirecionamento do tráfego
Spoofing (IP e DNS)	- Impedir o redirecionamento do tráfego - Criar regras contra IP spoofing no firewall (prevenir pacotes entrando com endereço privado de origem)
Vulnerabilides de aplicações em ambiente Web	- Refazer os filtros de entrada e saída de dados, para evitar SQL Injection e XSS. - Implementar verificação SOP (Same Origin Policy) - Implementar tokens para evitar CSRF - Implementar um Web Application Firewqall
Recusa de Serviço (Denial of Service)	- Configurar o firewall para impedir SYN flood - Detectar e mitigar ataques Smurf - Utilizar serviços como o CloudFlare para mitigar ataques de DDoS

Contramedidas

Exploração de Falhas	- Atualizar os softwares da máquina - Utilizar programas menos conhecidos - Melhorar regras do IPS para detectar os exploits e payloads.
- Keylogger - Vírus - Cavalos de Tróia - Worms - Spywares	- Anti-vírus corporativo com Internet Security -Firewall local (pessoal) - Anti-spywares - HIDS -Chkrootkit ou ferramenta similar

Contramedidas

- Rootkits	
Ataques Wireless	- Utilizar chave WPA2-PSK complexa, se possível usar WPA2-ENTERPRISE junto com um servidor Radius - Utilizar um certificado nos clientes - Ocultar a rede sem fio - Realizar um controle de acesso por MAC - Separar rede pública da administrativa por VLANs - Utilizar um WIPS (Wireless Intrusion Prevention System) - Evitar o uso de wi-fi em redes desconhecidas