

Marcos Flávio Araújo Assunção

Honeypots e Honeynets

Visual Books

Sumário

Prefácio	15
Conceitos Básicos	17
Definição	18
Princípios de Engenharia Social	19
Sistemas de Detecção de Intrusos	21
Network Intrusion Detection System	21
Detecção Baseada em Assinatura	22
Detecção Baseada em Anomalia	23
Host Intrusion Detection System	24
Segurança por Obscuridade	25
Honeypots	27
Riscos e Aspectos Legais dos Honeypots	27
Localização dos Honeypots	28
Tipos de Honeypots	29
Serviços de Alta Interação	29
Serviços de Baixa Interação	30
Objetivos dos Honeypots	30
Honeypots de Pesquisa	30
Honeypots de Produção	31
Honeynets	31
Honeynets GEN I e GEN II	32
Honeynet Real	32
Principais Componentes de uma Honeynet Real	33
Servidores/Computadores	33
Switch/Access Point	33
Cabos	33
Periféricos	33
Roteador	34
Firewall	34
IDS	34
Honeynet Virtual	35

Vmware	36
VirtualBox	36
VirtualPC	37
Criando uma Nova Máquina Virtual no Virtual PC	38
Centralização de Logs	43
Honeytokens	44
Honeywall	45
Tipos de Firewalls	45
Zona Desmilitarizada	46
Instalando o Iptables	47
Regras do Iptables	47
Chains	48
Tabelas	48
Utilização de Chains	50
Criando Novos Chains	52
Definindo um Alvo	53
Utilizando o NIDS Snort	54
Instalação do Snort no Linux	54
Instalação do Snort no Windows	55
Configuração do Snort	57
Serviços	58
DHCP	58
DNS	60
Registro de Recursos	62
Criando Zonas com o Servidor de Nomes BIND	63
VPN	65
Outros Serviços	70
Servidor HTTP – Apache ou IIS	70
Servidor de FTP – Proftpd ou IIS	70
Softwares	73
Deception Toolkit	73
Honeyd	74
KFSensor	78
Visualizando Informações de Log	80
Visualizando e Alterando Assinaturas de Ataque	83
Specter	85
Configurando Usuários	86
Visualizando Incidentes	87

Valhala Honeypot	89
Menu Opções	92
Alertar Tentativas de Invasão por E-mail	92
Enviar os Logs para o Servidor	93
Portas do Modo Console	93
Salvar Logs no Diretório	93
Atualizar as Configurações pelo Servidor	94
Limpar a Tela de Logs a cada X Linhas	94
Habilitar Portas Extras	94
Apagar Tela de Logs ao Enviar E-mail	94
Tocar Som ao Capturar Tentativas	94
Desabilitar Portas-padrão de Trojans	95
Iniciar com o Windows	95
Automonitorar	95
Modo Oculto	95
Banner Padrão das Portas Extras	95
Menu Configurar	95
Servidor WEB	96
Servidor FTP	98
Servidor Finger	102
Servidor POP3	103
Servidor SMTP	106
Servidor Telnet	107
Servidor TFTP	110
Servidor Proxy	112
Modo Console	113
PatriotBox	114
Ativando os Serviços	115
Configurando Serviços	117
Utilizando Scripts Personalizados	119