Faculdades Reges – Ribeirão Preto

MSc. Eng. Ali Faiez Taha

USP – Ribeirão Preto

aftaha@cirp.usp.br

18 de Abril de 2016

Segurança em Servidores Linux

Administração, manutenção e proteção do Sistema Operacional, Softwares e Serviços de Rede.

- **Necessidade básica**
- **Conexão à Internet**
- **Acessos não autorizados**
- **HACKERs e CRACKERs**

O quê proteger ?

- Arquivos e Dados da empresa
- Integridade
- Privacidade
- Disponibilidade
- Recursos
- Reputação

Proteger-se contra o quê ?

- **Diversos tipos de ataques**
- Roubo de senhas, de dados pessoais
- Fraudes, invasões, falsificação de documentos
- **BUG & Backdoors**, falha de autenticação
- **Falha de Protocolo**, **roubo de informações**
- Negação de serviços, **intrusão,** **rootkits**
- ***Scanners***, vulnerabilidades de Softwares, etc...
- Vírus e outras pragas
- Engenharia Social

Administração de recursos dos usuários

- Seleção adequada de **senhas.**
- Administração das contas de usuários.
- ACLs e utilização de recursos.
- Métodos de autenticação.
- Contas inativas, sem senha, administrativas, temporárias.
- Dados dos usuários, Backups, etc...

Segurança do Sistema de Arquivos

- Arquivos com SUID/GUID
- Shell Scripts com SUID
- ACLs - Access Control Lists
- Dispositivos de Input/Output
- Sistemas de arquivo Read Only
- NFS - Network File Systems
- Compartilhamento de arquivos

Controle do Sistema de arquivos

Detalhes da partição /dev/sda1 (no arquivo /etc/fstab):

/dev/sda1 /home xfs defaults, rw, nosuid, nodev, noexec

Onde:

- **defaults**: Permite quota, escrita e leitura e **SUID** na partição
- **quota: Quotas para usuários**
- **noquota**: Sem quotas na partição
- **nosuid**: Proíbe acesso de **SUID/SGID**
- **nodev**: Não cria caracteres ou dispositivos especiais na partição
- **noexec**: Não executa binários
- **ro: Somente leitura**
- **rw**: **Leitura e escrita**
- **suid**: **SUID/SGID - Root como usuário e como grupo**

Atributos e permissões especiais

SUID - utilizado em arquivos executáveis quando se deseja que o programa seja executado com os previlégios de seu dono.

- **chmod u+s arquivo**

SGID - mesma função do **SUID bit**, mas é aplicado ao grupo, ou seja, o programa é executado com os privilégios do grupo a que pertence.

- **chmod g+s arquivo**

Sticky bit - utilizado em diretórios compartilhados entre vários usuários. Diretórios com o **stick bit** ligado permite que qualquer usuário crie arquivos, mas os outros usuários não poderão remover estes arquivos.

- **chmod +t documentos**

Localização de arquivos com SUID e SGID

- **Arquivos com SUID root**:
- **find / -user root -perm -4000 -print**

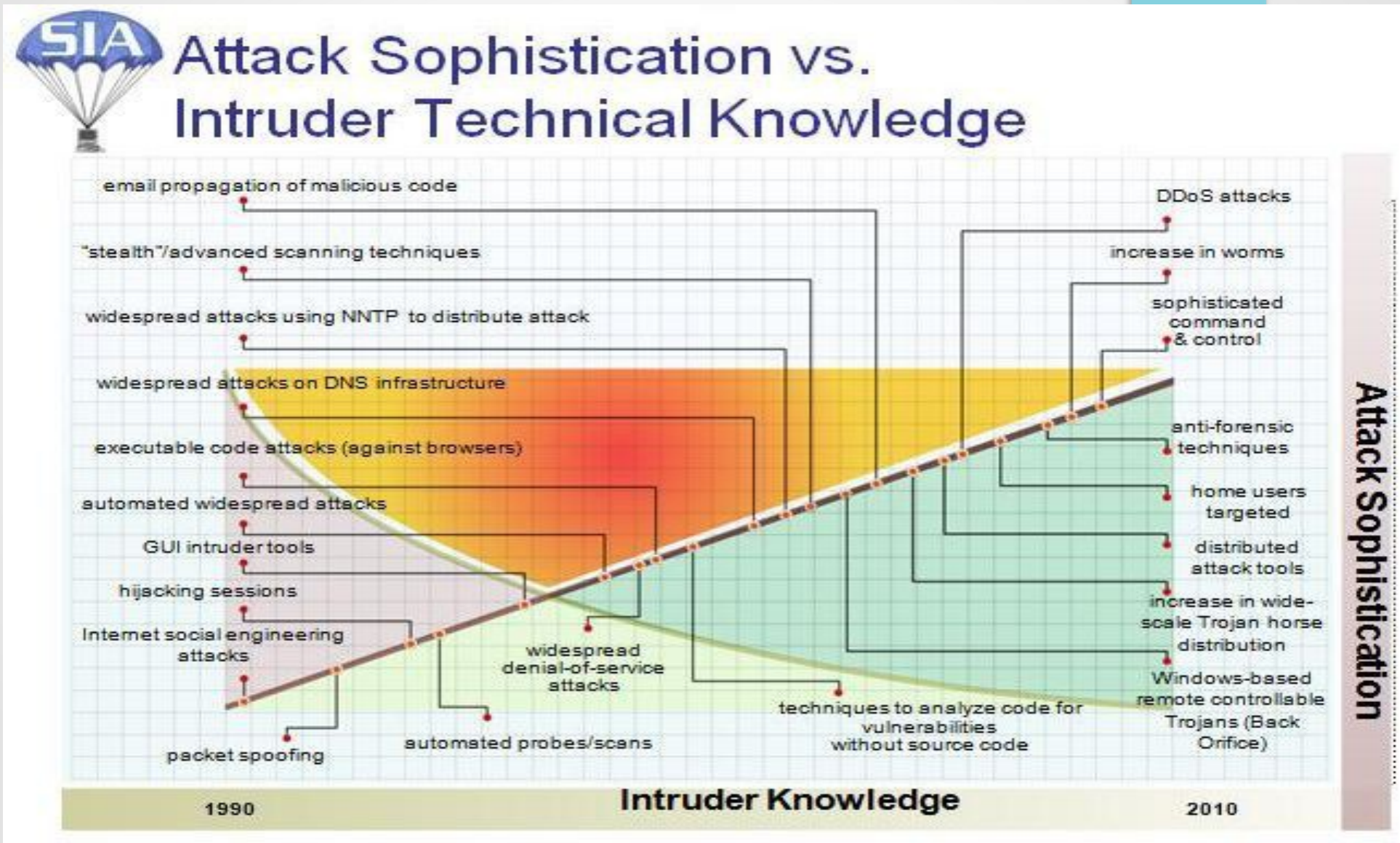
Arquivos com SGID root:

- **find / -group root -perm -2000 -print**

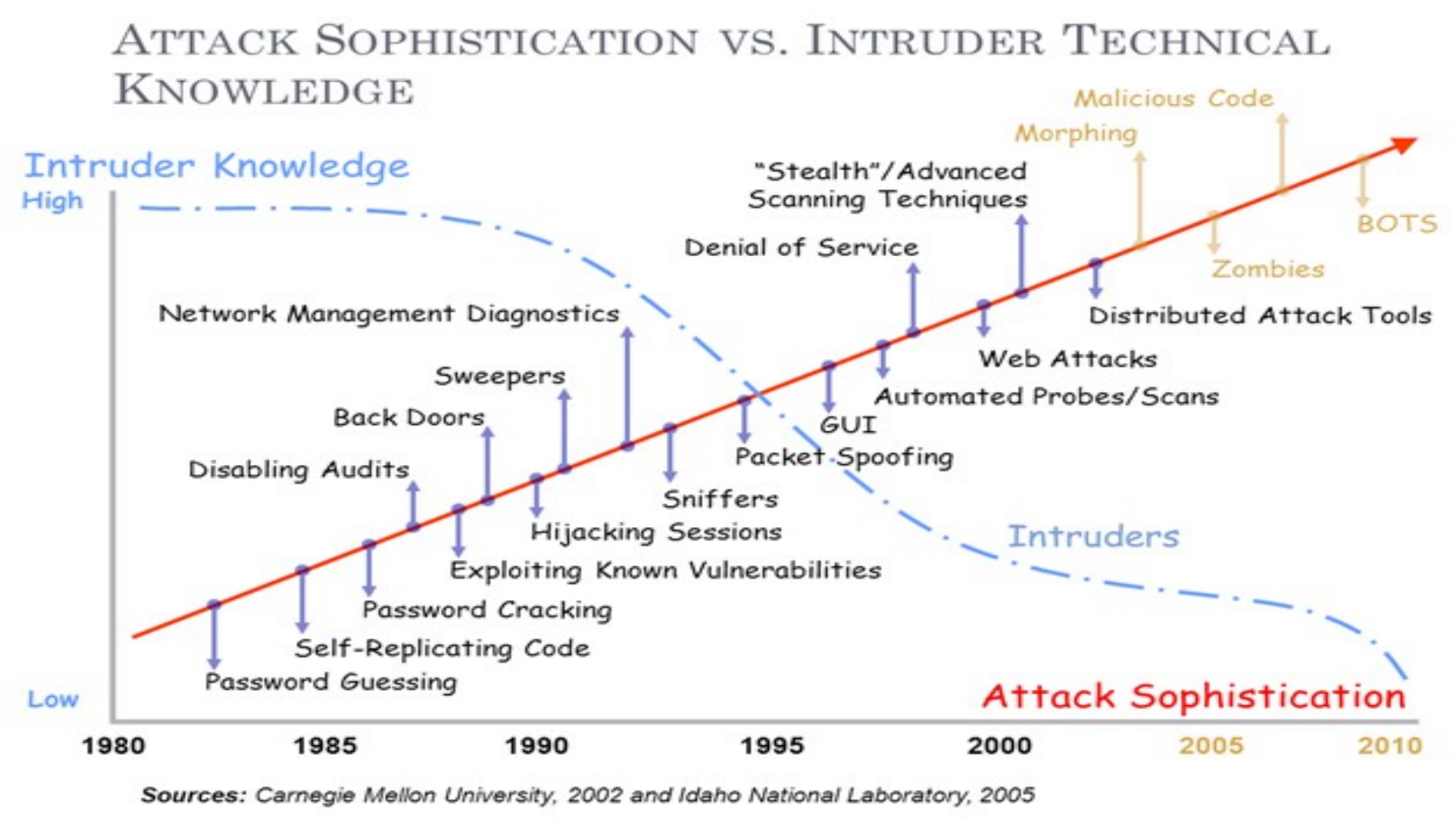
Arquivos com SUID e SGID:

- **find / -perm -4000 -o -perm -2000 -print**
- **Arquivos sem dono: find / -nouser -print**
- **Arquivos sem grupo: find / -nogroup -print**

Sofisticação dos ataques



Sofisticação dos ataques



Monitoração do servidor

- Fazer a monitoração constante de usuários, discos, serviços de rede, softwares instalados, comportamento do servidor, memória, arquivos de senhas, permissões, logs, logs, logs, logs...

Integridade do servidor

- Alteração em Sistema de Arquivos e Softwares instalados

  auditar com Tripwire
- Serviços de rede estranhos

  ferramentas www.sectools.org

Rootkits

- **Kits que escondem os processos e dão poderes de root.**
- **Difícil de detectar e de remover.**
- **Compromete o S.O e não deixa rastros.**
- **Remove evidências em arquivos de logs.**
- **Instala backdoors para acesso futuro.**
- ***Esconde atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede, etc.***
- **Mapeia potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede.**
- **Captura informações da rede onde o computador comprometido está localizado, pela interceptação de tráfego.**

Cavalo de Troia

Trojan Dropper: instala outros códigos maliciosos, embutidos no próprio código do trojan.

Trojan Backdoor: inclui backdoors, possibilitando o acesso remoto do atacante ao computador.

Trojan DoS: instala ferramentas de negação de serviço e as utiliza para desferir ataques.

Trojan Destrutivo: altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.

Trojan Clicker: redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.

Trojan Proxy: instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.

Trojan Spy: instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.

Trojan Banker ou Bancos: coleta dados bancários do usuário, através da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados. É similar ao Trojan Spy porém com objetivos mais específicos.

Trojan Downloader: instala outros códigos maliciosos, obtidos de sites na Internet.

Soluções para todos os problemas

- **Monitorar tudo, sempre.**
- **lsof -mostra arquivos em uso, donos, conexões de rede, etc...**
- **fuser – identifica processos usando arquivos e sockets.**
- **netstat - mostra conexões de rede, tabelas de roteamento, protocolos em uso, etc.**
- **strace – ferramenta para *debug* e monitoração de chamadas do sistema.**
- **tcpdump – analisa tráfego de rede.**
- **Outras... www.sectools.org**
- **Abuse das ferramentas chkrootkit e rkhunter**

Monitoração da Rede de Dados

- **Mapeie sua rede e conheça os serviços em execução.**
- **Analise o tráfego utilizando ferramentas apropriadas.**
- **Utilize nmap, nessus e procure por portas de conexão abertas.**
- **Identifique assinaturas de tráfego de rede, use o *snort*.**
- **Mapeie os serviços e respectivas vulnerabilidades.**
- **SNMP – Gerenciamento de equipamentos de rede.**
- **Conheça os *honeypots* .**
- **Utilize um Firewall e limite as conexões de rede.**
- **Cuidado com os ataques Denial of Service:**
- ***http://www.cert.br/docs/whitepapers/ddos/***

Segurança no Linux

- **Escolha uma distribuição que lhe facilite a vida.**
- **Cuide do seu Linux. Conheça as recomendações de segurança.**
- **Instale *APENAS* os pacotes e serviços que vai utilizar.**
- **Utilize ferramentas apropriadas para monitorar o servidor e os serviços de rede. Checksecurity é uma delas.**
- **Feche as portas TCP/IP que não utiliza e restrinja o acesso.**
- **Acompanhe os tutoriais How-to para configurar o Linux**
- **Mantenha o Linux atualizado.**
- **Tenha sempre um Backup e seja um pouco Hacker também.**

Ferramentas para segurança

- **Auditoria, port scanners, sniffers de rede, hackers tools, segurança de infra-estrutura, WEB online, atualização de Softwares e correção de bugs, Forense e recuperação de dados, Softwares Anti-vírus, Ataques, Honeypots, etc.**
- **Www.yolinux.com/TUTORIALS/LinuxSecurityTools.html**
- **Debian Administrator's Handbook : www.debian.org/doc/books**
- **Www.sectools.org**
- **Insecure.org/tools/tools-pt.html**
- **Www.cert.br**
- **Www.linuxsecurity.com**
- **Www.ugu.com**

Administração do Linux

- **Atualização do S.O. - Será que precisa recompilar o Kernel e todos os programas fontes do Linux ?**
- **Fontes seguras de Softwares – conheça a origem dos Softwares que utiliza.**
- **Atualização e aplicação de *patches* de segurança – fique atento pois tem muitas falhas em Softwares.**
- **Analisar os diversos tipos de vulnerabilidades – Um dia você fica craque e faz um Software a prova de falhas.**
- **Atenção aos alertas pelas comunidades de segurança – Bons amigos e bons conhecimentos.**

Auditoria constante – pense nisso !!!

- **Uso de ferramentas IDS, HIDS, NIDS – Detectar tentativas de intrusão**
- **Firewall – Será que precisa mesmo num simples servidor ou é só para usar em Redes ?**
- **Limitar acessos – Quem pode se conectar ao servidor ?**
- **Procure garantir a Integridade, Confidencialidade e Autenticidade dos dados**
- **Redes VPN – Circuito fechado entre as redes de uma empresa.**

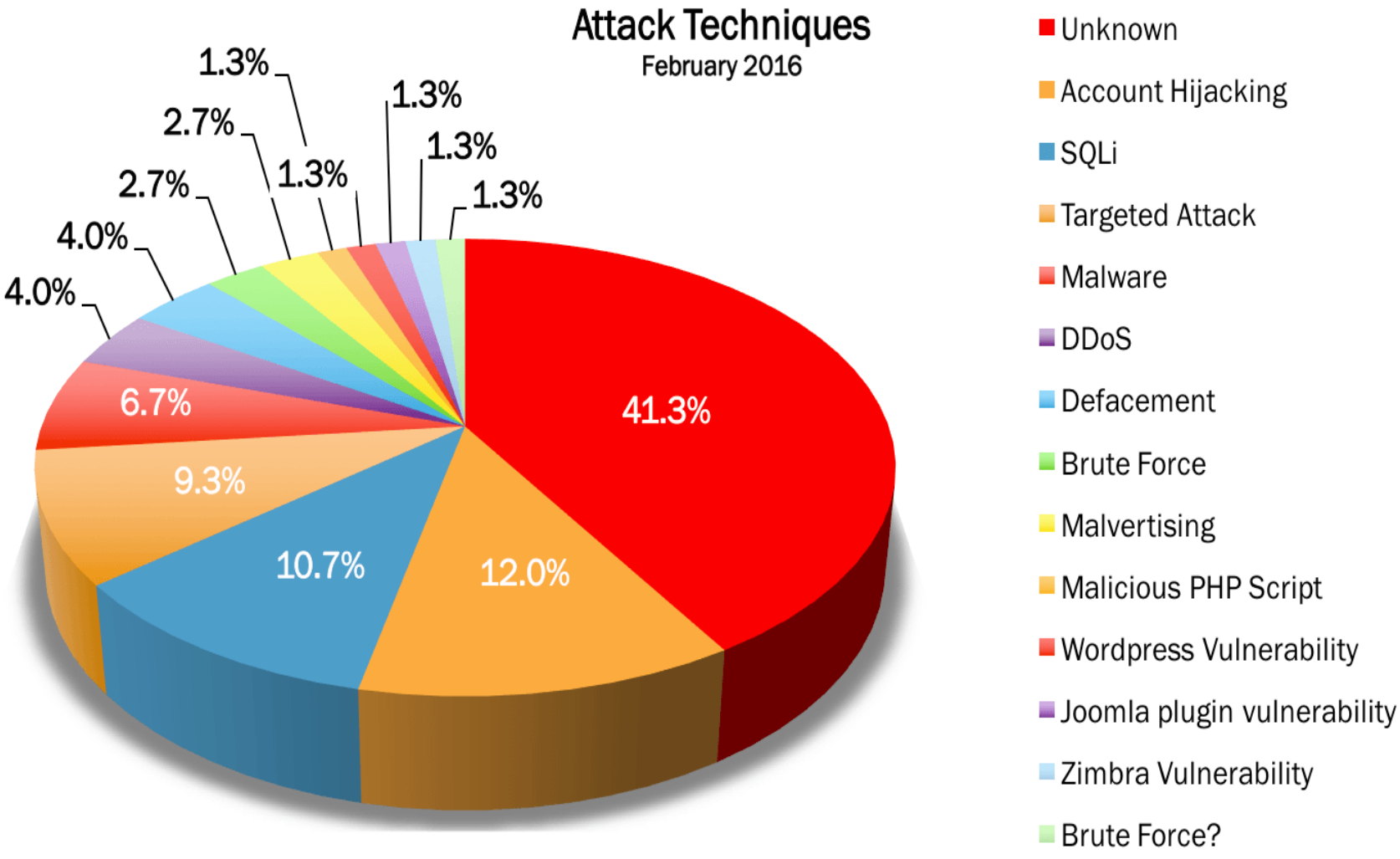
Site Security Handbook

- http://granito2.cirp.usp.br/SiteSecurityHandbook/
- **Este manual é um guia para desenvolvimento de políticas de segurança de computador e procedimentos para sites que têm seus sistemas na Internet. O propósito deste manual é proporcionar um guia prático aos administradores tentando tornar segura uma grande variedade de informações e serviços. Os assuntos abordados incluem os conteúdos de política e formação, tópicos técnicos de segurança de redes, e, também, reações a incidentes de segurança.**

Segurança da Informação

- Ser especializado em Segurança da Informação é uma boa opção.
- Muitos desafios e muito conhecimento técnico.
- Boas oportunidades no mercado de trabalho.
- Aprendizado constante.
- Vida social um pouco diferente.
- Conheça o Direito Digital.

Técnicas de ataques



http://www.hackmageddon.com/2016/03/24/february-2016-cyber-attacks-statistics/

Conclusão

- **Manter um S.O. Linux atualizado e totalmente seguro é um desafio. Os Softwares e protocolos apresentam falhas e erros de programação.**
- **Disponibilizar serviços na Internet exige cuidados e muita atenção, administração dos mesmos e constante preocupação.**
- **Utilizar ferramentas para segurança e proteção pode lhe tirar horas de sono e fomentar o aprendizado, ser um pouco diferente dos amigos e ser alvo de amigos do alheio.**
- **O nível de responsabilidade aumenta com a experiência e conhecimentos adquiridos, facilidades e domínio das tecnologias.**
- **Recomendável administrar o tempo e organizar as tarefas, orientar-se de acordo com as normas de segurança e boa conduta.**
- **Ética profissional, bom relacionamento com os amigos e profissionalismo.**
- **Conhecendo os Hackers, Crackers e suas atitudes você fica mais esperto e mais atento.**

Referências

- Www.cert.br
- http://www.cert.br/docs/
- http://www.cert.br/links/
- https://www.debian.org/security/
- http://csrc.nist.gov/publications/secpubs/curry.pdf
- https://en.wikipedia.org/wiki/Unix_security

  http://www.digitalattackmap.com
- http://map.norsecorp.com/#/

Aprender é mudar posturas - Platão

- A leitura faz ao homem completo; a conversa, ágil, e o escrever, preciso.
- Não há nada que faça um homem suspeitar tanto como o fato de saber pouco.

Francis Bacon