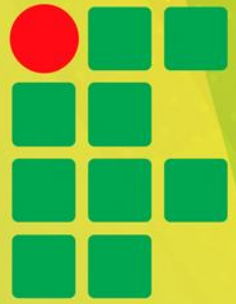
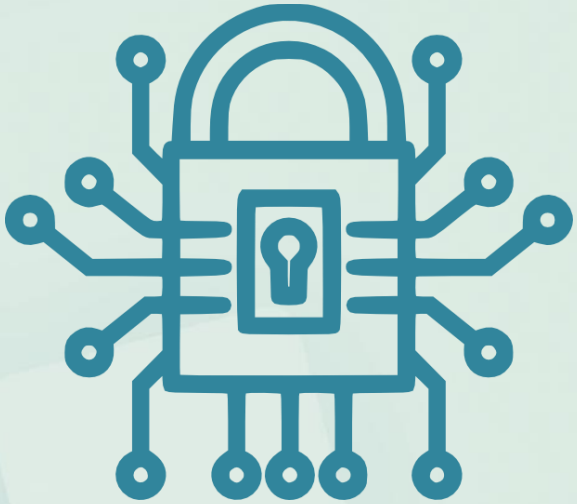


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação



Principais ameaças virtuais

Da atualidade

Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

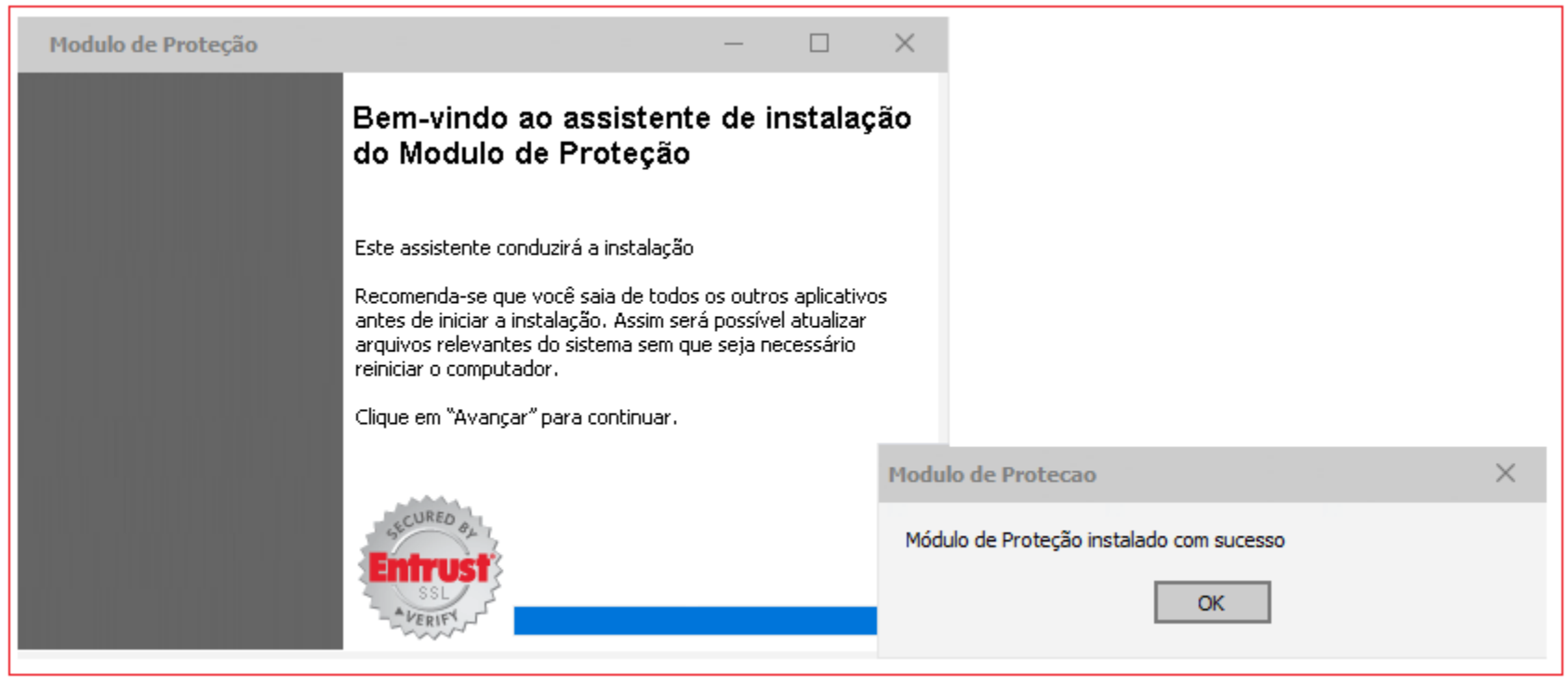
CAMUBOT:

Ataque Financeiro no Brasil

7.1. Camubot

- Ao contrário dos tradicionais trojans bancários, o CamuBot **não foca em ficar escondido, muito pelo contrário. Ele fica bem visível**, utilizando a logomarca do banco fraudado, **dando a impressão de que é um software de segurança do próprio banco**. Para ganhar a confiança da vítima, ele leva o usuário a crer que é necessária uma atualização da aplicação bancária e neste processo instala o Trojan.

7.1. Camubot


Modulo de Proteção
Bem-vindo ao assistente de instalação do Modulo de Proteção
Este assistente conduzirá a instalação
Recomenda-se que você saia de todos os outros aplicativos antes de iniciar a instalação. Assim será possível atualizar arquivos relevantes do sistema sem que seja necessário reiniciar o computador.
Clique em "Avançar" para continuar.
Modulo de Protecao
Módulo de Proteção instalado com sucesso
OK

7.1. Como funciona o Camubot?

- Os hackers do CamuBot começam com algum reconhecimento básico de informações para encontrar empresas que façam parte de um determinado banco.
- Em seguida, eles ligam para a pessoa que provavelmente teria as credenciais da conta bancária da empresa.

7.1. Como funciona o Camubot?

- Para efetivar o ataque, os invasores se identificam como funcionários do banco e instruem a vítima a procurar uma determinada URL para **verificar se o módulo de segurança dele está atualizado**. É claro que a verificação de validade é negativa, e os invasores **enganam a vítima para instalar um "novo" módulo de segurança**.

7.1. Como funciona o Camubot?

- Como parte de sua rotina de infecção, o CamuBot grava dois arquivos na pasta %ProgramData% Windows para estabelecer um módulo proxy no dispositivo. O nome do executável não é estático e muda em todos os ataques. Em seguida, **ele se adiciona às regras do firewall para parecer confiável**.

7.1. Como funciona o Camubot?

- Para se comunicar com o dispositivo infectado, o CamuBot estabelece um **proxy SOCKS baseado no Secure Shell(SSH).** A biblioteca de links dinâmicos (DLL) do módulo SSH é uma ferramenta gratuita que foi obtida via GitHub. O arquivo DLL é denominado “% TEMP% \ Renci.SshNet.dll”.

7.1. Como funciona o Camubot?

- Através do módulo proxy instalado os invasores estabelecem um túnel bidirecional de portas de aplicativos do dispositivo do cliente para o servidor. **Este túnel permite que os invasores direcionem seu próprio tráfego através da máquina infectada e usem o endereço IP da vítima ao acessar a conta bancária comprometida.**

7.1. Como funciona o Camubot?

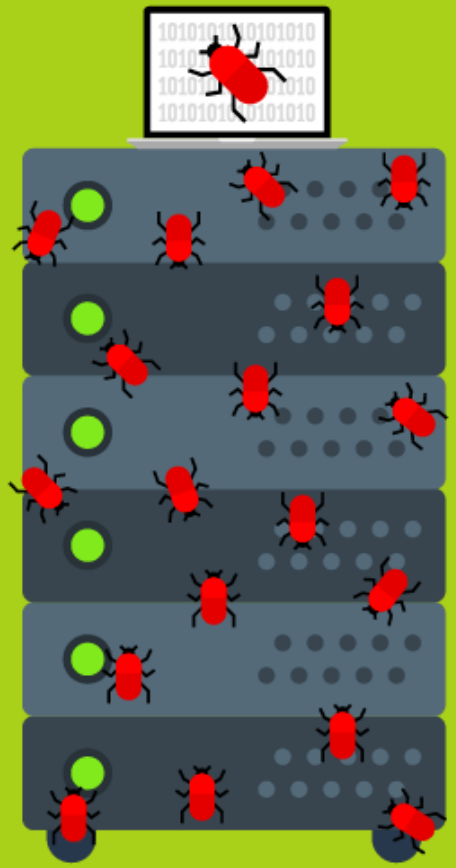
- Feita a instalação, uma tela pop-up **redireciona a vítima para um site de phishing**, idêntico ao do banco da vítima. A vítima é orientada a fazer login em sua conta, portanto, sem saber, **envia as credenciais para o invasor.**

- TIPOS -

mais comuns

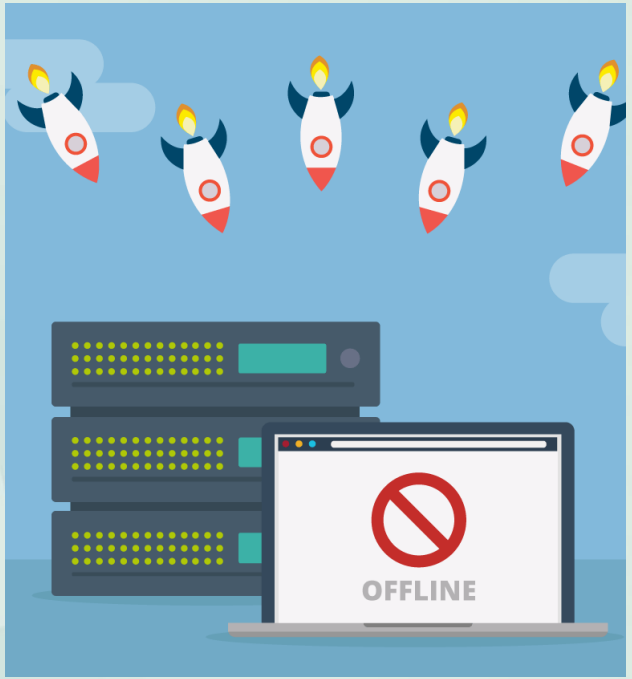
de ataques

DDoS



8.1. Ataques de Negação de Serviço

- Qualquer empresa pode ser alvo em potencial para ataques DDoS. Os afetados, geralmente, sofrem paralisações, levando à perda financeira e à degradação da reputação.



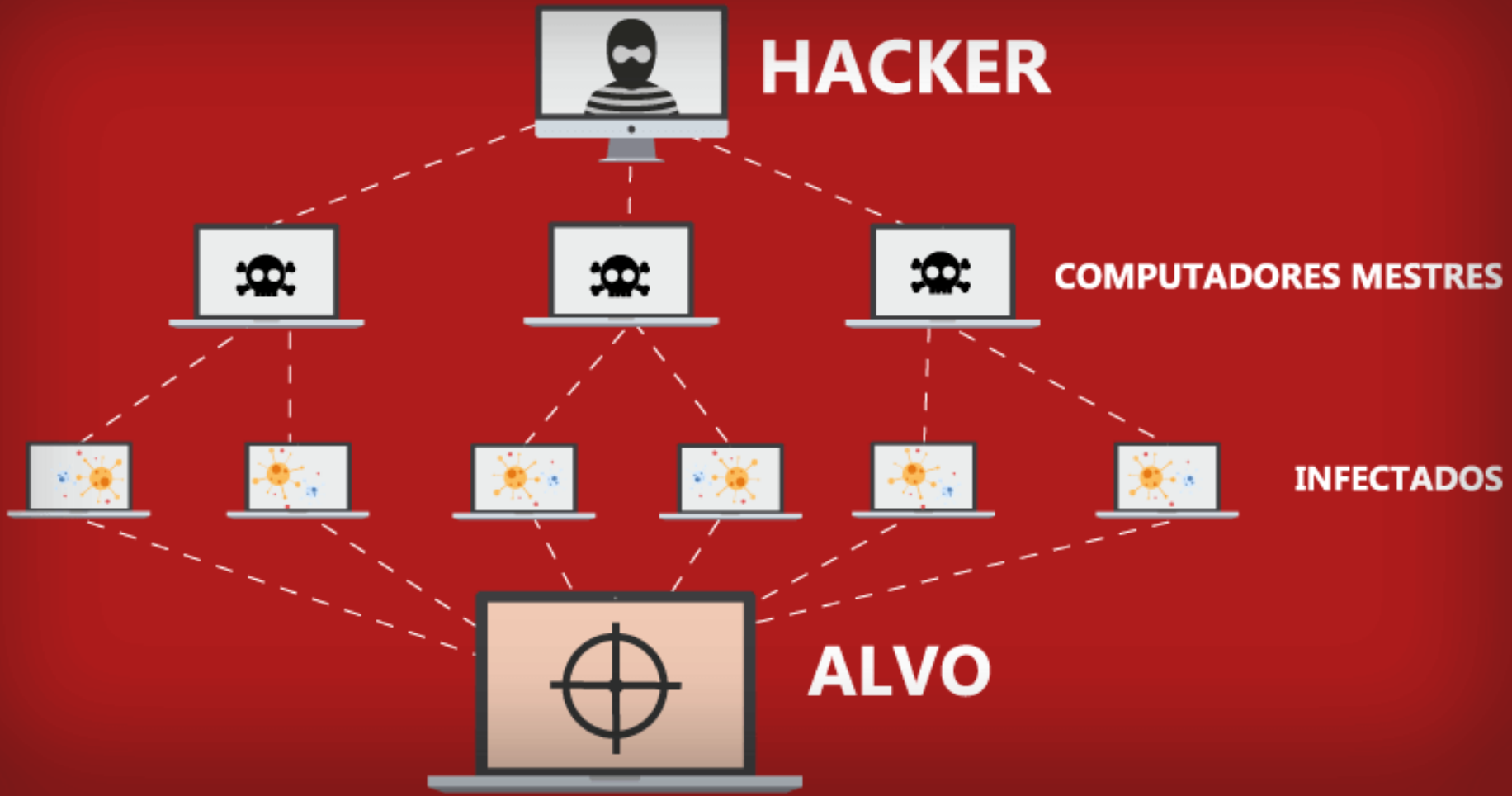
8.2. Dos e DDoS

- Por serem muito parecidos, muitas pessoas confundem os ataques DoS com os DDoS. A principal diferença entre os dois é na forma com que eles são feitos. Enquanto o ataque DDoS é distribuído entre várias máquinas, o ataque DoS é feito por apenas um invasor que envia vários pacotes.

8.3. Como funciona o DDoS?

- Um ataque DDoS é iniciado a partir de vários dispositivos comprometidos, geralmente distribuídos globalmente.

- Como o termo indica, a negação de serviço distribuída significa que ela **recusa o serviço a um usuário legítimo**.


HACKER
COMPUTADORES MESTRES
INFECTADOS
ALVO

8.4.1. Tipos: Ataques Volumosos

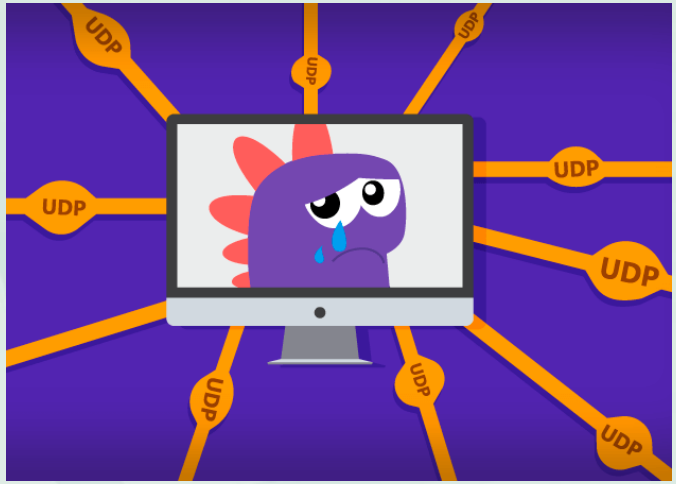
- Os ataques volumosos são, de longe, o tipo mais comum de ataques DDoS. Embora sejam caracterizados por uma enorme quantidade de tráfego (às vezes superior a 100 Gbps), eles não exigem uma grande quantidade de tráfego a ser gerada pelos próprios hackers.

8.4.1. Tipos: Ataques Volumosos

- Ataques volumosos baseados em reflexão direcionam um serviço enviando solicitações legítimas para um servidor DNS ou NTP usando um endereço IP de origem falsificado. Quando os servidores DNS ou NTP respondem à solicitação legítima, eles acabam servindo ao endereço de origem da solicitação, que por acaso é o endereço IP falsificado.

8.4.2. Tipos: UDP Flood

- O UDP Flood funciona em um princípio bastante básico. Os atacantes enviam um grande grupo de pacotes UDP para as portas aleatórias do servidor de destino. O servidor tem que responder a todos eles.

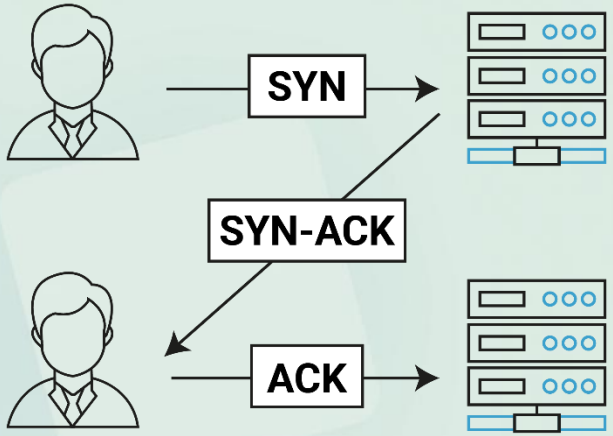


8.4.3. Tipos: NTP Flood

- No NTP Flood os invasores enviam pacotes válidos, porém falsificados, de NTP (Network Time Protocol) a um alvo de destino. Tudo acontece a uma taxa muito alta de pacotes originados de um grupo muito grande de endereços de IP.
- Como estas solicitações parecem ser verdadeiras, os servidores NTP da vítima continuam tentando responder à grande quantidade de solicitações recebidas.

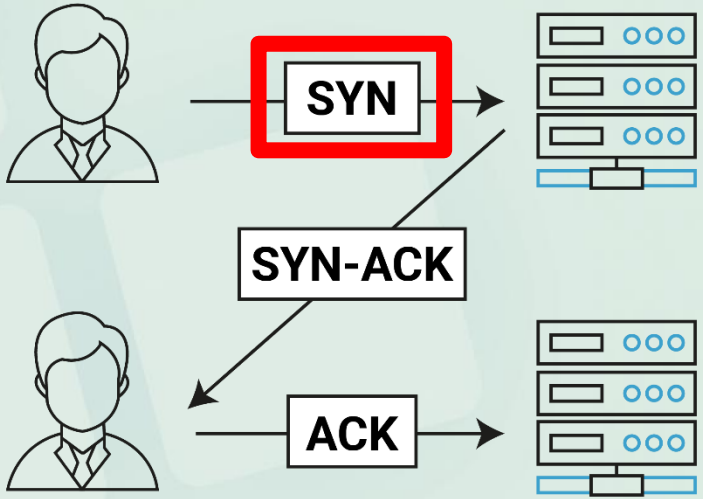
8.4.4. Tipos: SYN Flood

- Os ataques DDoS do tipo SYN Flood **afetam diretamente o processo de comunicação TCP de três vias.** Esse processo é popularmente conhecido como **“Aperto de Mão de Três Vias”** (Three-Way Handshake, do inglês).



8.4.4. Tipos: SYN Flood

- O SYN Flood **acontece quando o atacante envia pacotes SYN para o alvo**, como um servidor de destino. Só que esses envios acontecem a partir de IPs falsos, que podem estar mascarados na operação.



8.4.4. Tipos: SYN Flood

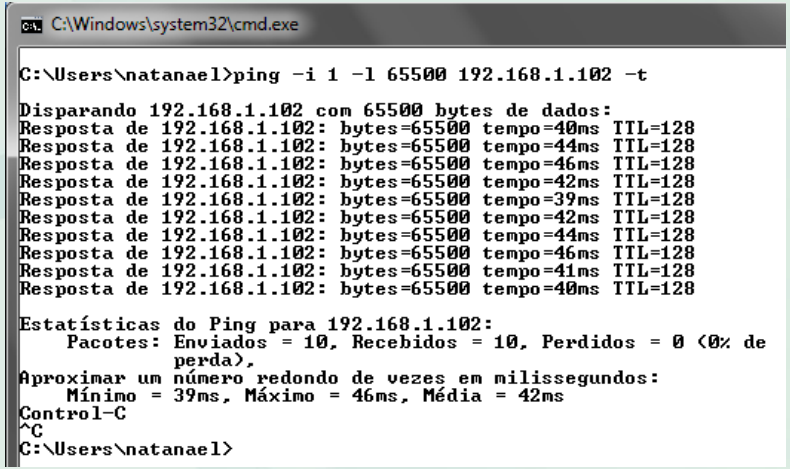
- Na repetição desse processo, a memória de conexão do servidor entra em colapso por não conseguir armazenar e processar os pacotes recebidos. E, **sem resposta, o sistema se torna inacessível, inviabilizando o seu acesso para qualquer usuário.**

8.4.5. Tipos: VOIP Flood

- Esse tipo de ataque DDoS é uma variação do UDP Flood. Mas em vez de bombardear portas aleatórias, o atacante envia um número gigantesco de solicitações falsas, originadas de vários IPs diferentes, especificamente **atingindo protocolos do tipo VoIP**.

8.4.6. Tipos: POD (Ping of Death)

- Também conhecido como Ping da Morte, nessa situação, o atacante envia a quantidade máxima de pacotes de dados do que os tipos de IPs conseguem suportar.



8.5. DDoS do futuro

- Antigamente, alguns cibercriminosos vendiam seus serviços de ataques DDoS. Eles deram um passo além e, hoje, vendem **botnets que fazem o serviço por conta própria**.

- Isso significa que hackers amadores têm acesso facilitado a ferramentas mais poderosas e simples de usar.

8.6. Como se proteger?

- Esteja preparado para todos os casos;
- Faça um investimento em largura de banda;
- Entenda o perfil de fluxo de tráfego do seu site/sistema;
- Disponha de um sistema de detecção de ataques de DDoS

8.6. Como se proteger?

- Esteja preparado para todos os casos;
- Faça um investimento em largura de banda;
- Entenda o perfil de fluxo de tráfego do seu site/sistema;
- Disponha de um sistema de detecção de ataques de DDoS

Obrigado!
Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano