BELLA
Building the Europe Link to Latin America

Conectando la investigación y educación europea y latinoamericana

Curso: Tratamento de Incidentes de Segurança da Informação

Prática 03: Ferramentas

Este roteiro de atividades visa exercitar o uso de ferramentas que auxiliam o trabalho no dia a dia do time de resposta a incidentes

Parte 01: Ataque de Força Bruta no SSH

Nesta atividade iremos praticar um tipo de ataque contra nosso próprio servidor virtual buscando entender como o ataque é feito para compreender melhor a visão do lado da defesa.

Ataques do tipo força bruta (ou sua ramificação, ataques de dicionários) são pautados nas boas escolhas dos parâmetros para ser enviados ao serviço e do uso de uma ferramenta para automatização dos testes. Dessa forma, faça um ataque de força bruta no SSH da máquina virtual, enquanto analisa os LOGs do serviço para entender como esse tipo de ataque é registrado no sistema.

1. Crie uma *wordlist* contendo possíveis usuários (por exemplo: *root*, *admin*) e outra contendo possíveis senhas (por exemplo: *123456*, *bahia, vitoria, qwerty*)

1.1. Busque criar *wordlists* que contenham as credenciais corretas e incorretas, a fim de analisar quando houve sucesso ou não

2. Faça o ataque utilizando as *wordlists* criadas por você no passo 1.

2.1. Caso queira utilizar o Hydra um possível comando é mostrado abaixo:

```
$ hydra -L wordlist_usuarios -P wordlist_senhas ssh://<ip_servidor>
```

EXTRA: Como seria um ataque em uma página web usando Hydra?

Parte 02: Análise de LOGs de Serviços

Considere que você trabalha mantendo um servidor que tem hospedado site com Wordpress e o acesso é feito via SSH. Você suspeita de ter tido comprometimento do servidor de alguma forma.

Baixe os arquivos *ssh.log* e *wordpress.log* e investigue o que ocorreu nesses serviços. Atente-se para entender completamente o que é reportado nos arquivos de LOGs para ser informações o suficiente para responder perguntas como as abaixo e muitas outras:

- Aconteceu algum ataque? Se sim, qual tipo de ataque?
- Se houve ataque, quem realizou esse ataque?
- Se houve ataque, quando começou? Quando acabou? Quanto durou?
- Houve comprometimento dos serviços? Se sim, quando?

Dicas: utilize o comando **grep** para filtrar o conteúdo dos arquivos e **awk** para exibir apenas os dados desejados. Procure identificar os padrões que caracterizam erros, ataques ou mau uso do sistema.

Boa prática! Em caso de dúvidas, não hesite em consultar os instrutores.