Fundamentos de Segurança Informática

Tarefas para as semanas #2 e #3 (com início em 25/10 e 1/11)

As tarefas a serem realizadas nas semanas #2 e #3 têm como objetivo principal garantir que a fase de arranque da organização da UC é concluída: formação de grupos e acesso ao gitlab. Como tal, serão avaliadas de forma agregada.

Como segundo objetivo pretende-se familiarizar os estudantes de FSI com o mundo do "vulnerability reporting" e os conceitos de vulnerabilidade, exploit, ataque, etc.

Como ponto de partida sugere-se a leitura do FAQ de apresentação do programa CVE disponível em: https://cve.mitre.org/about/faqs.html bem como a explicação do programa Common Weakness Enumeration da mesma instituição https://cwe.mitre.org/about/index.html.

O objetivo da tarefa é que cada grupo escolha uma vulnerabilidade existente na base de dados CVE, para a qual exista um exploit documentado, e produza uma curta caracterização da mesma.

Para este efeito devem consultar-se, entre outras, as seguintes referências web:

- https://cve.mitre.org
- https://www.exploit-db.com
- https://nvd.nist.gov
- https://www.cvedetails.com/
- https://cwe.mitre.org

Tarefas a realizar na Semana #2

1 - Formação do grupo e registo do grupo no Moodle

```
- esta tarefa permitirá depois à equipa docente criar um repositório git para o grupo
- isso será feito no final da semana #2/início da semana #3
```

2 - Escolha de um identificador CVE-AAAA-NNNN para CVE a explorar na semana #3

```
- este identificador deve ser registado no ficheiro https://git.fe.up.pt/fsi/fsi2122/cve/-/blob/main/choices.txt na linha correspondente ao grupo
- não são permitidos CVE repetidos, pelo que cada grupo deve verificar que o CVE inserido não ocorreu anteriormente
```

Tarefas a realizar na Semana #3

1 - Caracterização do CVE escolhido na semana #2:

- Identificação: descrição geral da vulnerabilidade, incluindo aplicações/sistemas operativos relevantes (max 4 itens com 20 palavras cada)
- Catalogação: o que se sabe sobre o seu reporting, quem, quando, como, bug-bounty, nível de gravidade, etc. (max 4 itens com 20 palavras cada)
- Exploit: descrever que tipo de exploit é conhecido e que tipo de automação existe, e.g., no Metasploit (max 4 itens com 20 palavras cada)
- Ataques: descrever relatos de utilização desta vulnerabilidade para ataques bem sucedidos e/ou potencial para causar danos (max 4 itens com 20 palavras cada)

2 - Discussão do CVE escolhido na semana #2 CVE na aula TP

3 - Registo da caracterização anterior em `LOGBOOK3.md` no repo gitlab do grupo.

Tarefas adicionais

Como preparação para as aulas seguintes, os grupos devem preparar um ambiente para execução dos tutoriais SEED: https://github.com/seed-labs/seed-labs.

Existem diversas opções para este ambiente que podem ser utilizadas, mas recomenda-se a seguinte: https://github.com/seed-labs/seed-labs/blob/master/manuals/vm/seedvm-manual.md.

Os grupos devem também verificar que têm acesso à plataforma CTF em http(s)://ctf-fsi.fe.up.pt. O desafio SanityCheck não é para avaliação, e visa apenas demonstrar qual o formato de uma flag: a resposta encontra-se facilmente lendo as regras de funcionamento na plataforma.

Última alteração: quarta, 3 de novembro de 2021 às 09:27

◄ Funcionamento das Aulas TP e CTF

Ir para...

Tarefas para a semana #4 (com início em 8/11) ►

Portal de e-learning
Ajuda Moodle
Inovação Pedagógica