Instituto de Matemática e Estatística da USP

MAC0352 - Redes de Computadores e Sistemas Distribuídos - 1s2022

EP4
Definição de data, equipe e tópico até 8:00 de 24/5/2022 (DUPLA)

Prof. Daniel Macêdo Batista

1 Objetivo

O objetivo desta avaliação é permitir a exploração de alguma vulnerabilidade em redes de computadores, mostrando qual a falha de programação que levou à vulnerabilidade e como essa falha pode ser corrigida.

Apesar de ser chamado de "EP", vocês não precisam escrever novos códigos. Utilizar códigos de *exploits* e *patches* existentes é recomendado mas é necessário que esses códigos sejam compreendidos para que possam ser explicados na aula. Simplesmente usar o *exploit* e o *patch* como um *script kiddie*[1] não é o objetivo deste trabalho.

2 Tarefas

1. Escolha alguém para fazer o trabalho junto. **O trabalho não pode ser feito individualmente**. Deve ser feito em dupla. Caso haja uma quantidade ímpar de pessoas matriculadas, 1 único grupo terá três pessoas.

2. Escolha um tópico para fazer o seu trabalho. Ou seja, pesquise por exemplo no DuckDuckGo ou em fóruns de segurança de redes de computadores[2] sobre vulnerabilidades que foram descobertas em serviços de redes a partir de 2019 e que tenham soluções. As vulnerabilidades podem ser em qualquer camada da arquitetura Internet.

3. Estude a vulnerabilidade, e sua solução, do ponto de vista de programação, e avalie se sua equipe conseguirá demonstrar. Caso vocês não consigam, volte para a Tarefa 2.

[1] `https://en.wikipedia.org/wiki/Script_kiddie`
[2] Recomendo que a busca seja feita em `https://cve.mitre.org/cve/search_cve_list.html`

4. **Apresente o tópico para o professor no fim de alguma aula para ouvir a opinião dele**. Se ele disser que esse tópico é muito simples ou que não tem relação com redes de computadores, volte para a Tarefa 2. Tópicos enviados por e-mail para o professor ou para a monitora serão ignorados. Tópicos colocados diretamente no fórum da disciplina sem ter passado pelo aval do professor também serão ignorados.

5. Escolha uma data para apresentar o seu trabalho e escreva no fórum da disciplina, na *thread* de título "Informações do EP4 (Até as 8:00 de 24/5/2022)", as seguintes informações:

   Tópico (Número do CVE e um título que resuma a falha)

   Integrantes da equipe

   Data de apresentação

6. Prepare uma apresentação de **no máximo 20 minutos** em que sua equipe consiga explicar a falha, explorá-la ao vivo na sala de aula, aplicar a correção na falha, tentar explorá-la depois da correção e não conseguir, mostrando que a correção funcionou. Note que a explicação da falha tem que apresentar brevemente o serviço/sistema/protocolo que vocês vão explorar, e mostrar, no código-fonte, onde está a falha. O *patch* que corrige o problema também precisa ser apresentado a nível de código-fonte. Recomenda-se fortemente que toda a demonstração da falha seja feita utilizando virtualização, por exemplo via `Xen`, `VirtualBox`, ou `docker`, e que pacotes sejam capturados usando o `tcpdump` ou o `wireshark`. **Tentativas de explorar serviços reais da USP ou de outro local serão punidas com nota ZERO na disciplina. Vocês devem apresentar a exploração em algum computador de vocês e em uma rede virtualizada durante a demonstração na sala de aula.**

As vulnerabilidades escolhidas para apresentar precisam ter sido descobertas a partir de 2019, mas **não** podem ser as seguintes:

- CVE-2019-11043
- CVE-2019-15107
- CVE-2019-15606
- CVE-2019-20916
- CVE-2019-3553
- CVE-2019-5432
- CVE-2019-6111
- CVE-2019-9740
- CVE-2019-9741
- CVE-2020-13849
- CVE-2020-25684
- CVE-2020-36049

- CVE-2020-5202
- CVE-2020-7247
- CVE-2020-8128
- CVE-2020-8277
- CVE-2020-8492
- CVE-2020-8794
- CVE-2020-9283
- CVE-2021-21241
- CVE-2021-29513
- CVE-2021-32640
- CVE-2021-33502
- CVE-2021-33880

3 Avaliação

Será usado o seguinte critério de avaliação:

- Explicação do serviço e da falha: 2,0
- Apresentação e explicação clara do problema no código-fonte do serviço: 2,0
- Apresentação e explicação do código-fonte do *exploit* que explora a vulnerabilidade: 1,0
- Demonstração da vulnerabilidade ao vivo: 2,0
- Apresentação e explicação do código-fonte do *patch* que corrige a vulnerabilidade: 2,0
- Demonstração de que com o *patch* a vulnerabilidade deixa de existir: 1,0

Perguntas serão feitas pelo professor após a apresentação a fim de definir as notas finais de cada um dos itens acima. Notem que não é necessário programar um novo exploit e nem um novo patch para a vulnerabilidade. Vocês podem usar algo que já existe mas devem deixar claro quem são os autores.

Punições:

- **Escrita das informações no fórum da disciplina fora do prazo**: quem escrever as informações fora do prazo, mesmo que por 1 segundo, terá nota zero no EP, será considerado que ele não foi entregue e a MF será zero também.
- **Não apresentação do tópico para o professor**: quem não apresentar o tópico para o professor na sala de aula, antes de escrever no fórum da disciplina, terá nota zero no EP, será considerado que ele não foi entregue e a MF será zero também.
- **Divisão injusta na apresentação**: se durante a apresentação não houver uma divisão justa para cada integrante da equipe falar/demonstrar algo, a nota final do EP será a nota dada pelo professor dividida pela quantidade de integrantes da equipe.

4 Datas

- Escrita das informações no fórum da disciplina na *thread* de título “Informações do EP4 (Até as 8:00 de 24/5/2022)”: até 24/5 às 8:00. Lembrem que é necessário apresentar o tópico para o professor antes de escrever no fórum. Programe-se com antecedência.
- Dias para as apresentações (em cada dia poderá haver até 2 apresentações): 2/6, 7/6, 9/6, 21/6, 23/6, 28/6, 30/6, 5/7, 7/7 e 12/7.