MAC0352 - Redes de Computadores e Sistemas Distribuídos - 1s2021
EP4
Definição de data, equipe e tópico até 8:00 de 1/7/2021 (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* 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[1] sobre vulnerabilidades que foram descobertas em serviços de redes a partir de 2018 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.

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 ou no fórum da disciplina para o professor ou para o monitor serão ignorados.

5. Escolha uma data para apresentar o seu trabalho e escreva no fórum da disciplina (já há uma *thread* sobre isso lá, de título "Informações do EP4", basta responder) as seguintes informações:

[1] Recomendo que a busca seja feita em `https://cve.mitre.org/`

Tópico

Integrantes da equipe

Data de apresentação

6. Prepare um vídeo de, **no máximo, 20 minutos** em que sua equipe explica a falha, explora a mesma em computadores que vocês tenham acesso, aplica a correção na falha, tenta explorá-la depois da correção e não consegue, mostrando que a correção funcionou. Note que a explicação da falha tem que apresentar brevemente o serviço que vocês vão explorar, e mostrar, no código-fonte do serviço, 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 via `VirtualBox`, `Xen` ou `VMWare` 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.**

7. Coloque o vídeo no Google Drive e envie o link para o fórum da disciplina, na mesma *thread* do item 5 acima. Certifique-se de habilitar o compartilhamento do vídeo para que a turma, o monitor e o professor consigam acessá-lo.

As vulnerabilidades escolhidas para apresentar deverão ser aquelas descobertas a partir de 2018, mas **não** podem ser as seguintes:

- CVE-2018-1000224
- CVE-2018-10933
- CVE-2018-15473
- CVE-2019-11043
- CVE-2019-15107
- CVE-2019-9740
- CVE-2019-9741

3 Avaliação

Será usado o seguinte critério de avaliação:

- Explicação do serviço e da falha: 2,0
- Apresentaçao 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 no(s) seu(s) computador(es): 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 o vídeo ser exibido a fim de definir as notas finais de cada um dos itens acima. O monitor também dará notas para cada item e a nota final será a média entre a nota do professor e a nota do monitor. Notem que não é necessário codificar 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 no fim de alguma 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 no vídeo da 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 1/7 às 8:00. Lembre 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 3 apresentações): 29/7/2021, 27/7/2021, 22/7/2021, 20/7/2021, 15/7/2021, 13/7/2021, 8/7/2021, 6/7/2021 e 1/7/2021.
- Envio do link do vídeo no fórum da disciplina (na mesma *thread* de título "Informações do EP4"): até as 7:00 da manhã do dia da apresentação. Esse vídeo será apresentado no computador do professor por isso é importante que haja tempo hábil para o professor fazer o download. Se o envio do link não for feito dentro do prazo, ele terá que ser apresentado por compartilhamento de tela no computador de alguém da equipe. Mesmo nesse caso, com atraso, o link deverá ser colocado no fórum da disciplina. Se não for colocado até o horário dele ser apresentado, a nota final do EP será zero, será considerado que ele não foi entregue e a MF será zero também.