MAC0448/5910 - Programação para Redes de Computadores
EP4

Prof. Daniel Macêdo Batista

1 Objetivo

O objetivo desta avaliação é permitir aos alunos que eles explorem 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 patchs existentes é recomendado mas é necessário que esses códigos sejam compreendidos para que possam ser explicados em sala de 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 alunos, 1 único grupo terá três pessoas.

2. Escolha um tópico para fazer o seu trabalho. Ou seja, pesquise no google ou em fóruns de segurança de redes de computadores[1] sobre vulnerabilidades que foram descobertas em serviços de redes nos últimos 5 anos 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 você conseguirá demonstrar em sala de aula. Caso você não consiga, volte para a Tarefa 2.

4. Apresente o tópico para o professor no fim de alguma aula para ver 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 email para o professor serão ignorados.

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

   Tópico

   Integrantes da equipe

   Data de apresentação

[1] Recomendo que a busca seja feita em `https://cve.mitre.org/` `http://secunia.com/community/advisories/product/` e `http://secunia.com/community/advisories/vendor/`

6. Prepare uma apresentação de 25 minutos em que você 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 que você vai 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 o wireshark. **Tentativas de explorar serviços reais da USP ou fora da mesma serão punidas com nota ZERO na disciplina. Você deve apresentar a exploração em algum computador seu e em uma rede virtualizada durante a demonstração na sala de aula.**

Os tópicos que foram escolhidos por alunos nas últimas edições desta disciplina **não** poderão ser escolhidos este ano. São eles:

- Bug no processamento de imagens em programas da Mozilla (CVE-2012-3966)
- Vulnerabilities in Ruby on Rails Action Pack (CVE-2013-0156)
- Dropbear SSH Server denial of service (CVE-2013-4421)
- Ataque DoS sobre vulnerabilidade do NTP (CVE-2013-5211)
- Overflow na busca binária do SpiderMonkey (CVE-2013-5619)
- D-Link user agent backdoor (CVE-2013-6026)
- Heartbleed Bug (CVE-2014-0160)
- OpenSSL CCS Injection Vulnerability (CVE-2014-0224)
- Erro na manipulação de curingas no arquivo de configuração do OpenSSH (CVE-2014-2532)

3 Avaliação

- Explicação do serviço e da falha: 2,0
- Demonstração clara do problema no código-fonte do serviço: 2,0
- Apresentação e explicação do código-fonte do exploit que explora a vulnerabilidade: 1,0
- Apresentação 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.

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.
- 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.
- Divisão injusta na apresentação: se durante a apresentação não houver uma divisão justa para cada um 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: até 9/10 às 8:00
- Dias para as apresentações (em cada dia poderá haver até 2 apresentações): 24/11, 12/11, 10/11, 5/11, 3/11, 29/10, 27/10 e 22/10