Questão 1: Acabei de executar o comando **nmap moodle.unihacker.club**, por que não estou mais conseguindo acessar o Moodle?

Resposta: É muito provável que o seu ISP (Provedor de Internet) esteja monitorando e bloqueando atividades de varredura de portas (por scanning), como as realizadas pelo **nmap**.

O que posso fazer? Se você já foi bloqueado pelo seu ISP, você precisará **utilizar o navegador Tor**, **uma VPN (*Virtual Private Network*) ou ainda um servidor proxy externo**, para continuar tendo acesso ao **Moodle.UniHacker.Club**. O que aconteceu, provavelmente, foi o seguinte: o seu ISP bloqueou as conexões de saída para o endereço **moodle.unihacker.club**, suspeitando que você esteja realizando atividades potencialmente maliciosas contra o site. **Se você ainda não foi bloqueado pelo seu ISP**, você poderá utilizar opções menos intrusivas do **nmap**, como o parâmetros **-T** (para selecionar um template de temporização, de 0 a 5 - quanto mais alto mais rápido), **-F** (modo rápido - faz um scan em menos portas) e **-p** (para limitar o número de portas). Por exemplo, utilizar **-T2** (para um scan mais lento) e **-p U:53,137,T:20-25,80-100,44-600,990-995,8080,8081** (para um scan num subconjunto limitado de portas). Na prática, para resolver a questão que envolve um scan no Moodle, utilizando o **nmap**, você pode utilizar um comando como o apresentado a seguir (um scan mais lento em um subconjunto limitado de portas **U**DP e **T**CP).

nmap -T2 -p U:53,137,T:22,80,443,465,587,993,995,8080,8081 moodle.unihacker.club

Questão 2: Acabei de executar duas vezes o comando **nmap moodle.unihacker.club**, entretanto, as duas respostas foram diferentes, como ilustrado nas imagens (scan 1 e scan 2) a seguir. O que pode estar acontecendo?

scan 1 (nmap moodle.unihacker.club): saída do nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-13 12:43 -03
Nmap scan report for moodle.unihacker.club (200.132.136.124)
Host is up (0.034s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.59 seconds
```

scan 2 (nmap moodle.unihacker.club): saída do nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-13 12:44 -03
Nmap scan report for moodle.unihacker.club (200.132.136.124)
Host is up (0.035s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

Resposta: O firewall do servidor **moodle.unihacker.club** pode estar configurado para suspeitar de potenciais atividades exploratórios contra a porta SSH (22). Nesse caso, o acesso à porta 22 é bloqueado na segunda varredura de portas utilizando o **nmap**. O mesmo mecanismo pode estar ativo para as portas 80 (HTTP) e 443 (HTTPS). Entretanto, para estas portas, o limite para classificação de atividade suspeita pode, geralmente, ser maior. Em outras palavras, a execução de dois comandos **nmap**, sequenciais, ainda não é o suficiente para ativar o bloqueio da porta para o IP de origem da varredura de portas.
Eis um exemplo de configuração de um filtro de pacotes, como o IPTables, no Linux, para limitação de tentativas de conexão por intervalo de tempo. Vejam que, nessa configuração, se forem identificadas 3 tentativas de conexão (**--hitcount 2**) num intervalo de 20 segundos (**--seconds 20**), a origem das conexões será automaticamente rejeitada, como tcp-reset (**--reject-with tcp-reset**), pelo IPTables.

-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name SSH --rsource
-A INPUT -p tcp -m tcp --dport 22 **-m recent --rcheck --seconds 20 --hitcount 3** --rttl --name SSH --rsource -j REJECT **--reject-with tcp-reset**
-A INPUT -p tcp -m tcp --dport 22 **-m recent --rcheck --seconds 20 --hitcount 2** --rttl --name SSH --rsource -j LOG **--log-prefix "SSH brute force "**
-A INPUT -p tcp -m tcp --dport 22 **-m recent --update --seconds 20 --hitcount 2** --rttl --name SSH --rsource -j REJECT **--reject-with tcp-reset**
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

Questão 3: A pouco, executei um **nmap** e consegui acessar o Moodle. Agora, executei novamente o **nmap** e não consigo mais acessar o Moodle. Por que isto acontece?
Resposta: Há diferentes explicações para este comportamento. Uma das explicações, que pode estar relacionada com o firewall do sistema alvo, foi apresentada na resposta da questão 2. Uma segunda explicação para esse comportamento, supostamente estranho, entretanto corriqueiro, é o fato de ISPs (provedores de Internet) utilizarem firewalls, entre outros mecanismos de segurança, para detectar e barrar ações potencialmente maliciosas, como varreduras de portas

subsequentes. Por exemplo, boa parte dos firewalls e sistemas de detecção de intrusões em redes (*Network Intrusion Detection System*, ou NIDS) incorpora recursos como detectores de ataques de varredura de portas (*Port Scan Attack Detector*, ou PSAD), que são responsáveis pelo monitoramento, detecção e bloqueio de ações suspeitas, como as varreduras de portas com o **nmap**. Portanto, você pode estar sendo bloqueado pelo seu provedor de Internet, o que é algo bastante comum hoje em dia.