**GAC119 - REO 1: Análise de Vulnerabilidades**

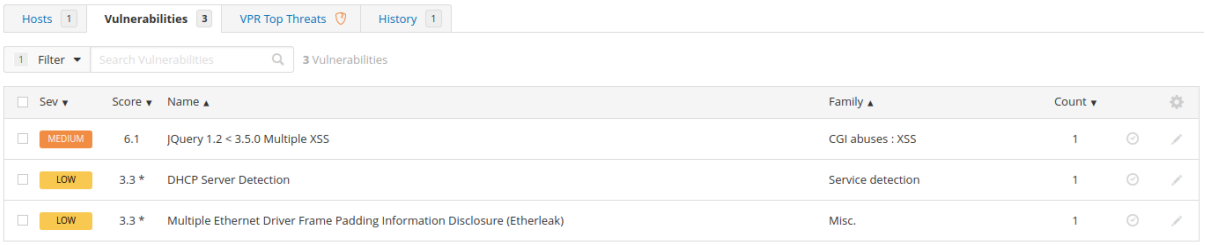
*Mateus Carvalho Gonçalves - 201810245*
*Pedro Antônio de Souza - 201810557*

## ANÁLISE 1

**Alvo:** Roteador wifi utilizado na residência de Mateus

**Descrição:** Essa análise de vulnerabilidades foi feita para examinar a segurança do roteador fornecido pela provedora de internet. A ferramenta Nessus foi escolhida para o escaneamento.

**Análise:** O escaneamento retornou mensagens de 25 categorias. Destas, 22 são de propósito informativo. Logo, o Nessus classificou 3 vulnerabilidades, listadas na figura abaixo.




A primeira, classificada como média e score 6.1, foi a identificação de um JQuery com versão maior ou igual a 1.2 e menor que 3.5.0. Esse fato torna possível diversos ataques XSS (cross site scripting). Na opinião dos autores, o diagnóstico feito pelo Nessus nesse caso é adequado

Também foi apontada a disponibilidade do serviço DHCP, o que foi pontuado como baixa. Porém, essa vulnerabilidade pode ser excluída, uma vez que é realmente um trabalho do dispositivo.

Finalmente, o Nessus também indicou a presença de um Etherleak, vulnerabilidade do tipo CVE que facilita ataques do tipo exploit. Ela foi classificada com severidade baixa e é sugerido contatar o provedor de internet para resolver o problema.

**ANÁLISE 2**

**Alvo:** Roteador wifi utilizado na residência de Pedro

**Descrição:** Análise de vulnerabilidades feita para examinar a segurança do roteador no IP 192.168.0.1. O aparelho é da marca TP-Link e modelo Archer C5. A ferramenta Nessus foi escolhida para o escaneamento.

**Análise:** O escaneamento apontou quatro vulnerabilidades e informações de 24 categorias distintas. Como a pode ser visto na figura abaixo, três vulnerabilidades foram categorizadas com nível médio de severidade e uma com nível baixo.

| Sev ▾ | Score | Name | Family | Count |
|---|---|---|---|---|
| MEDIUM | 6.5 | IP Forwarding Enabled | Firewalls | 1 |
| MEDIUM | 6.5 | Unencrypted Telnet Server | Misc. | 1 |
| MEDIUM | 5.3 | SMB Signing not required | Misc. | 1 |
| LOW | 3.3 * | DHCP Server Detection | Service detection | 1 |

Foi verificado que o equipamento possui um serviço de roteamento de IP habilitado. Contudo, essa detecção já era esperada pois esse serviço é responsável pela função desempenhada pelo equipamento. Dessa forma, pode-se classificar a vulnerabilidade como um falso-positivo.

Assim como na análise feita com o nmap, foi detectado um servidor Telnet sem criptografia. Esse serviço possibilita ataques do tipo man-in-the-middle para obter credenciais ou outras informações sensíveis. Portanto, essa vulnerabilidade é procedente. Recomenda-se que esse serviço seja substituído por um SSH a fim de garantir mais proteção à rede.

Além disso, foi identificada uma vulnerabilidade no SMB Server. Esse serviço, que é utilizado para fornecer acesso compartilhado a arquivos e impressoras, também pode facilitar ataques do tipo man-in-the-middle. Sendo assim, essa detectação é pertinente.

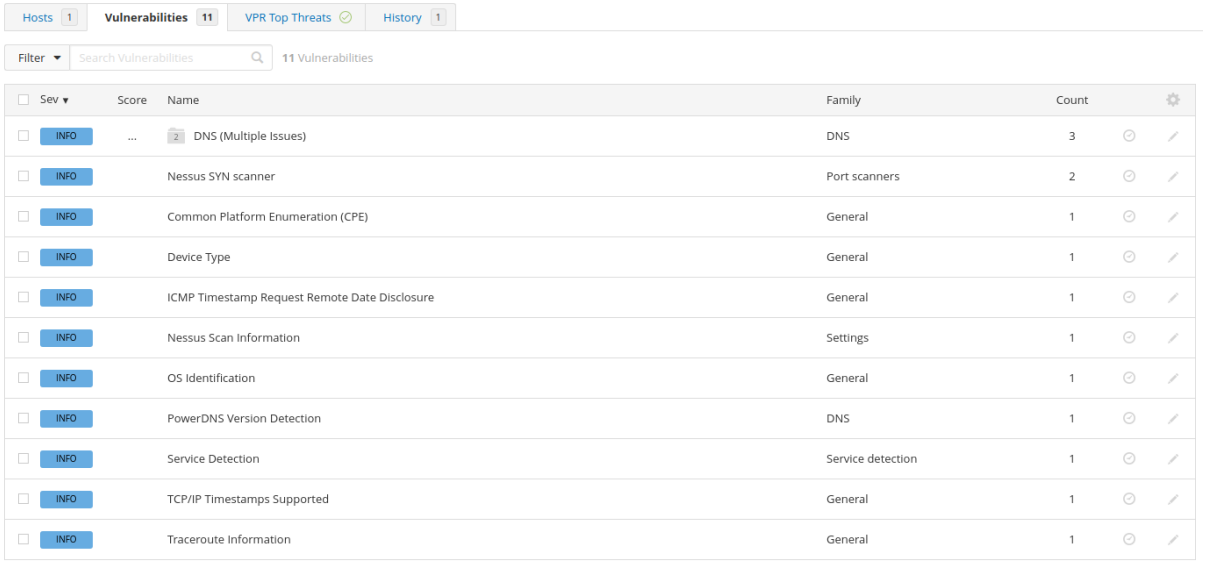
Por fim, como o equipamento é um roteador e sua tarefa principal depende da disponibilidade de um DHCP, a vulnerabilidade classificada como baixa também pode ser considerada um falso-positivo.

## ANÁLISE 3

**Alvo:** Servidor DNS da Namecheap Inc. (ns1.epizy.com).

**Descrição:** A análise de vulnerabilidades do servidor, cujo IP (107.189.11.47) foi extraído na Atividade 2 do REO 1, foi feita com intuito de descobrir mais sobre a segurança de serviços de hospedagem gratuitos da web. O servidor em questão hospeda uma aplicação web feita pela dupla em 2019, como parte da disciplina de Arquitetura de Computadores 2. A ferramenta Nessus foi escolhida para o escaneamento.

**Análise:** O escaneamento não encontrou vulnerabilidades, mas retornou informações de 11 categorias. Abaixo serão discorridas os principais dados levantados no escaneamento.



Hosts 1 | Vulnerabilities 11 | VPR Top Threats | History 1

Filter | Search Vulnerabilities | 11 Vulnerabilities

| Sev | Score | Name | Family | Count |
|---|---|---|---|---|
| INFO | ... | DNS (Multiple Issues) | DNS | 3 |
| INFO | | Nessus SYN scanner | Port scanners | 2 |
| INFO | | Common Platform Enumeration (CPE) | General | 1 |
| INFO | | Device Type | General | 1 |
| INFO | | ICMP Timestamp Request Remote Date Disclosure | General | 1 |
| INFO | | Nessus Scan Information | Settings | 1 |
| INFO | | OS Identification | General | 1 |
| INFO | | PowerDNS Version Detection | DNS | 1 |
| INFO | | Service Detection | Service detection | 1 |
| INFO | | TCP/IP Timestamps Supported | General | 1 |
| INFO | | Traceroute Information | General | 1 |

Em primeiro instante, percebe-se que o Nessus não encontrou nenhuma vulnerabilidade preocupante pois, como dito anteriormente, todos os resultados foram apenas informativos.

A primeira mensagem apresentada pela ferramenta diz respeito à detecção de um servidor DNS, o que obviamente era esperado, já que é a função da máquina. Ainda sobre isso, também foi possível identificar a versão do servidor: PowerDNS Authoritative Server 4.2.3. Pelo entendimento dos autores, isso não necessariamente é um problema, mas pode servir para identificar possíveis vulnerabilidades relacionadas à versão.

No geral, as informações levantadas foram bastante parecidas com o levantamento feito com nmap, como: sistema operacional, CPE, tipo de dispositivo, detecção de portas e serviços, traceroute, entre outras.

**ANÁLISE 4**

**Alvo:** Servidor DNS primário do provedor de  Internet (Vivo) de Mateus

**Descrição:** Análise feita com intuito de saber se o Nessus levantaria mais informações do que o nmap no levantamento de informações e vulnerabilidades do DNS da Vivo (IP 187.50.250.115).

**Análise:** O escaneamento não retornou nenhuma informação. Vale lembrar que foi utilizada a opção Basic Network Scan.