Governo do Estado de
RONDÔNIA
SETIC

Coordenadoria de Segurança
RELATÓRIO MENSAL
Abril/2021

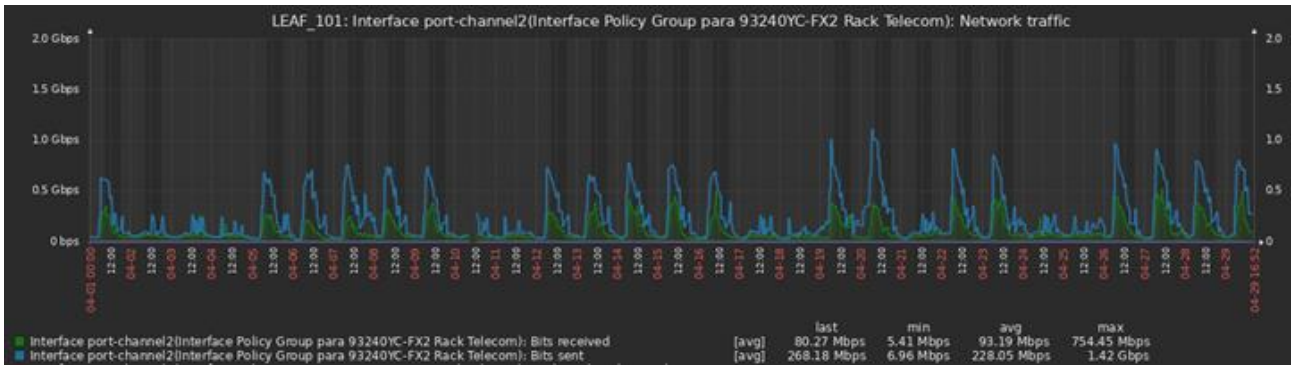
2021

Relatório Mensal - Abril/2021

Sumário

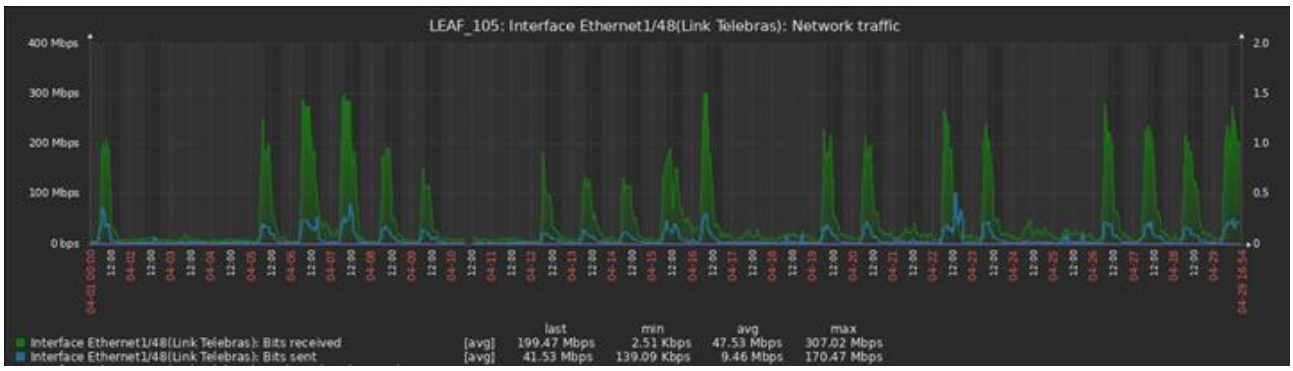
1. Tráfego de Rede

Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da DETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **107 TB** de informação trafegada no mês deste relatório.

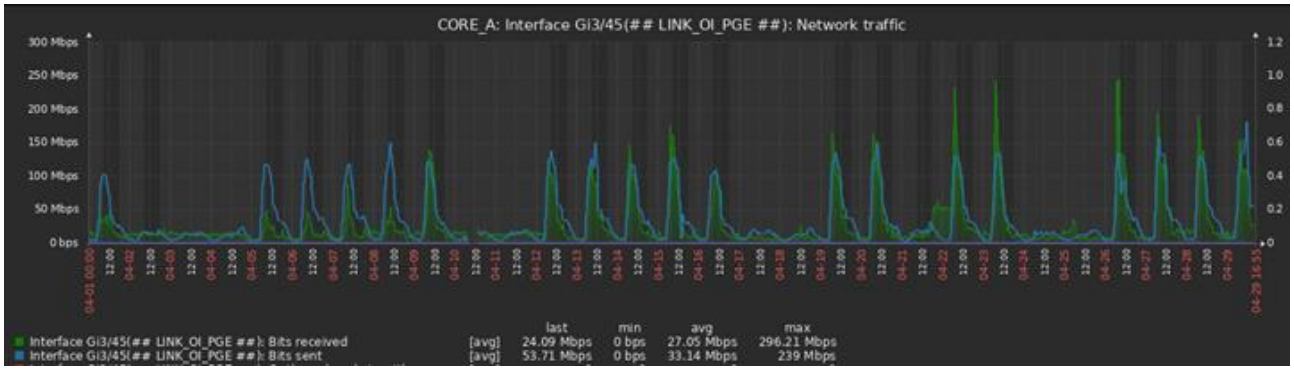


Monitoramento de tráfego Cores DETIC

Além disso, foram consumidos **39 TB** de tráfego da Internet, considerando acesso dos usuários à aplicações de Governo expostas na Internet e acesso a serviços pelo público geral.



Monitoramento de tráfego Link Telebrás



Monitoramento de tráfego Link Oi

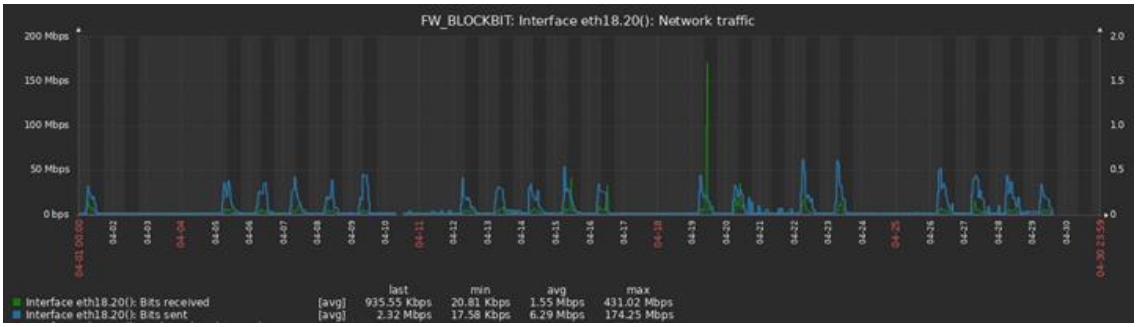
1.1 Consumo por Secretária

Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da DETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **6 TB** de informação trafegada no mês deste relatório por secretária.

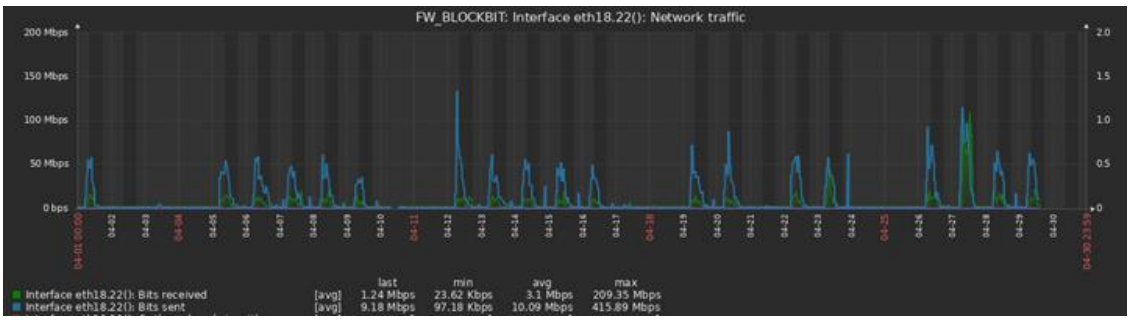
Dados refere-se as duas mais consumidoras deste mês.

Secretária DER/SEOSP: **2 TB**

Secretária SUGESP:**4 TB**



Monitoramento de tráfego DER/SEOSP



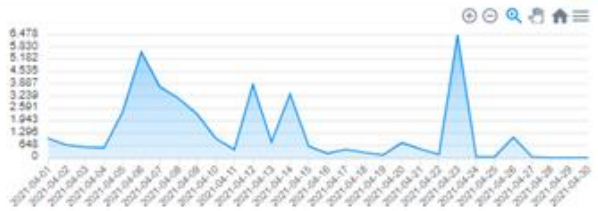
Monitoramento de tráfego SUGESP

2. Ataque

Vale à pena frisar que ainda não possuímos uma infraestrutura que nos garanta a segurança de dados, no que tange às tecnologias de proteção topo de linha no mercado de TI. Porém a ferramenta que utilizamos hoje registrou um total de **39.418** Ataques Registrados durante o mês do presente relatório.

Como contramedida para resolver o problema acima relatado, estamos aguardando a entrega de novos appliances de Firewall, adquiridos via comodato em nosso novo contrato de link's. Com os novos dispositivos, de um fabricante líder de mercado em segurança da informação, teremos uma proteção ativa de maior qualidade frente aos nossos serviços.

Top Categorias



#	Categoria	Hits
1	SNMP	11.807
2	PROTOCOL-SNMP	11.730
3	SERVER-WEBAPP	7.000
4	POLICY-OTHER	4.180
5	PROTOCOL-DNS	1.148
6	DNS	1.047
7	WEB_SERVER	897
8	SERVER-MAIL	630
9	SMTP	440
10	INDICATOR-SHELLCODE	411

Top Tipos de Classes

#	Tipo de Classe	Hits
1	Attempted Information Leak	26.367
2	Attempted Administrator Privilege Gain	4.122
3	Access to a Potentially Vulnerable Web Application	3.830
4	Web Application Attack	2.328
5	Potential Corporate Privacy Violation	1.414
6	Misc activity	993
7	Executable Code was Detected	421
8	Attempted User Privilege Gain	391
9	Potentially Bad Traffic	206
10	Detection of a Denial of Service Attack	45

Top Origens

#	Origem	Hits
1	172.16.32.82	17.633
2	172.16.50.3	6.054
3	177.128.118.198	2.407
4	185.215.113.36	1.037
5	10.9.0.8	822
6	138.219.49.202	648
7	179.253.180.169	541
8	143.198.112.48	492
9	143.198.120.235	487
10	179.252.63.157	452

Top Destinos

#	Destino	Hits
1	192.68.2.1	17.276
2	172.16.0.143	5.760
3	10.9.0.11	3.022
4	10.9.0.5	2.087
5	172.16.36.2	1.761
6	10.9.12.2	1.301
7	172.16.0.158	1.088
8	172.16.0.159	967
9	10.9.12.3	951
10	10.9.0.6	535

3. Vulnerabilidade

Trata-se das análises de vulnerabilidades realizadas em servidores de rede pertencentes ao Governo do Estado de Rondônia gerenciados ou hospedados pela SETIC, utilizando-se os softwares Nmap1 e OpenVAS2 .

Tais procedimentos se deram em decorrência das diretrizes da Coordenação de Segurança da Informação da SETIC, bem como da intenção de criar a Gerência de Prevenção e Respostas a Incidentes e a solicitação das equipes de Operações e DataCenter da Coordenação de Infraestrutura da SETIC.

O OpenVAS, ao analisar determinado alvo, classifica as vulnerabilidades encontradas em 3 (três) diferentes níveis de gravidade: **alto, médio** e **baixo**. Destaca-se ainda que apresenta também o nível denominado “log”, que objetiva trazer informações sobre o alvo, não sendo objeto de discussão neste relatório.

Ao todo, foram analisados **24** (vinte e quatro) servidores de rede, dos quais **6 (25%)** apresentaram **alto** nível de gravidade, **11 (45,8%)** apresentaram **médio** nível, **5 (20,8%)** apresentaram **baixo** nível, conforme classificação do OpenVAS, destacando-se ainda **que 2 (8,3%)** servidores não apresentaram **nenhuma** vulnerabilidade, pelo fato de estarem com todas as portas fechadas.

Importante ressaltar que nas análises, alguns servidores que apresentaram alto nível de gravidade também apresentaram gravidades de nível médio e baixo, bem como alguns servidores que apresentaram médio nível de gravidade também apresentaram gravidades de nível baixo.

No decorrer das análises o OpenVAS detectou 287 notificações, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **7 (2,4%) de alto nível, 260 (90,6%) de médio nível e 20 (7%) de baixo nível.**

Nos testes realizados foram identificadas diversas vulnerabilidades, entretanto não se descarta outras que porventura não foram detectadas ou que surjam futuramente.

3.1 Quantidade de Servidores

Utilizando-se do OpenVAS, considerando sua classificação das vulnerabilidades em 3 (três) diferentes níveis de gravidade (alto, médio e baixo) foi possível analisar **24** (vinte e quatro) servidores de rede, dos quais **6 (25%)** apresentaram alto nível de gravidade, **11 (45,8%)** apresentaram **médio** nível, **5 (20,8%)** apresentaram **baixo** nível, conforme classificação do OpenVAS, destacando-se ainda que **2 (8,3%)** servidores não apresentaram **nenhuma** vulnerabilidade, pelo fato de estarem com todas as portas fechadas, conforme "Gráfico 1 – Nível de gravidade" abaixo:

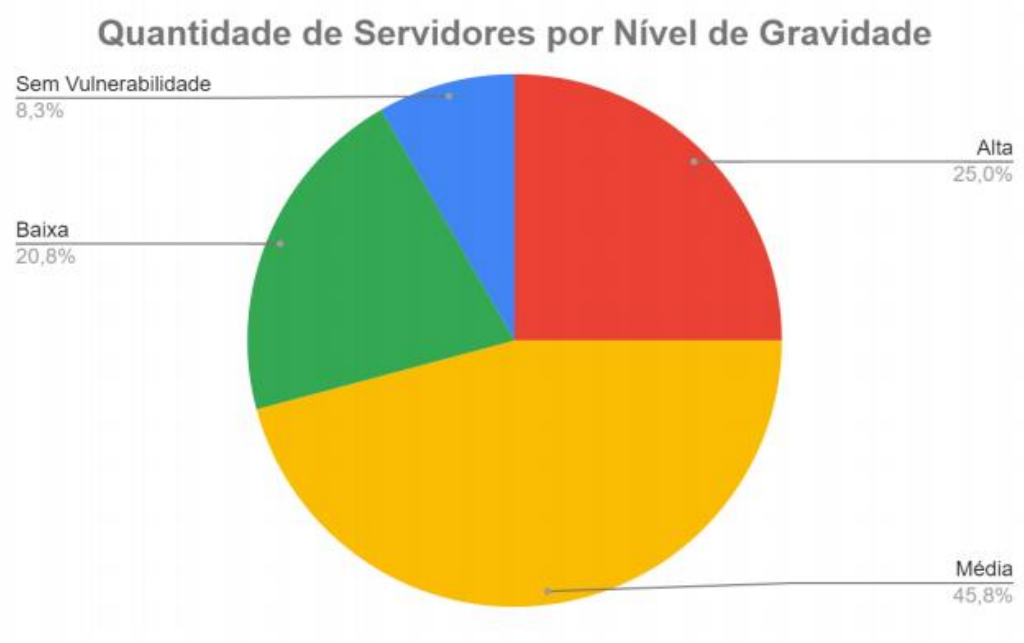


Gráfico 1 – Quantidade de Servidores

3.2 Quantidade de Vulnerabilidades

No que diz respeito às notificações apresentadas pelo OpenVAS, destacam-se que foram detectadas **7 (2,4%) de alto nível, 260 (90,6%) de médio nível e 20 (7%) de baixo nível.**

Gráfico 2 – Quantidade de Vulnerabilidade

3.3 Categoria de Vulnerabilidades

Além disso, com base nos relatórios do OpenVAS, procurou-se categorizar as principais vulnerabilidades encontradas nos servidores de rede que foram analisados, criando as seguintes categorias: Web (PHP, HTTP, APACHE); Chaves de Segurança (SSL, TLS, OPENSSH); Acesso Remoto (RPC, FTP, DCE, TCP); Informações do Sistema (TCP TIMESTAMPS); Compartilhamento de Arquivos (SMB WINDOWS); Banco de Dados (MariaDB, SQL); e Backup File.

Dessa forma, procurou-se destacar a vulnerabilidade mais crítica de cada servidor e classificá-la em uma dessas categorias, com objetivo de facilitar a identificação do segmento que se encontra mais vulnerável na rede, exigindo atenção e adoção de políticas de correção e mitigação de falhas e problemas de segurança. Sendo assim, foi possível perceber que a maioria das vulnerabilidades encontradas estão vinculadas à Acesso Remoto (13 servidores) Chaves de Segurança (17 servidores) e Informações do Sistema (20 servidores).

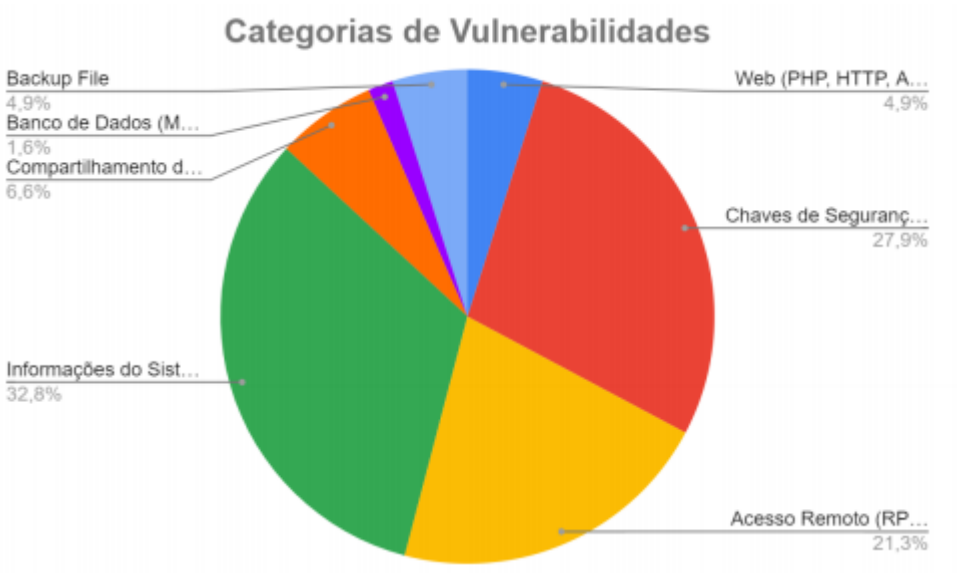


Gráfico 3 – Categoria de Vulnerabilidade

4. Ações Corretivas

Após a realização das análises e produção dos relatórios, contendo informações conjuntas do Nmap e OpenVAS, estes foram enviados ao setor de Datacenter, responsável por realizar as correções aplicando as medidas necessárias. Tal procedimento foi determinado pela Coordenação de Infraestrutura da SETIC, considerando que esse setor que administra os servidores que foram analisados.

Os relatórios foram enviados por meio de chamados abertos pelo GLPI (https://atendimento.detic.ro.gov.br), sistema de controle de requisições da SETIC, sob os protocolos de número:

2021040196 - 2021040199 - 2021040201 - 2021040202 - 2021040203 - 2021040204 - 2021040206 - 2021040346 - 2021040348 - 2021040349 - 2021040350 - 2021040351 - 2021040352 - 2021040354 - 2021040355 - 2021040357 - 2021040699 - 2021040640 - 2021040641 - 2021040642 - 2021040643 - 2021040832 - 2021040835 - 2021040837

No APÊNDICE – Controle de análises, encontra-se uma tabela contendo informações sobre as referências, endereços de IP, datas das análises, softwares utilizados para realizá-las, nível de gravidade, as principais falhas detectadas, a vinculação de endereços internos ou externos quando identificados, o número do chamado no GLPI e sua data de abertura.

Superintendência do
Estado para Resultados

Governo do Estado de
RONDÔNIA

Wiki.DETIC

Plataforma de Documentação Operacional e Gerencial dos Serviços da EpR

Conheça: wiki.detic.ro.gov.br