



Relatório Breaking Enigma

Trabalho realizado:

1191830 Rui Marques

Junho, 2021

**Docente(s)/Orientador(es)**

Marcelo Santos (MEF)

Vladir Vicente (VLV)

**Unidade Curricular**

Segurança de Aplicações e Dados

Indice

[1. Introdução 3](#_Toc89869245)

[2. Desenvolvimento 3](#_Toc89869246)

[3. Programa 3](#_Toc89869247)

[4. BIBLIOGRAFIA 5](#_Toc89869248)

# Introdução

O objetivo deste trabalho foi criar um programa que atacasse uma “hash” com o auxílio de uma “wordlist” e “plugboard” fornecidas.

Essa “hash” correspondia a uma das palavras fornecidas na “wordlist”, misturada com um “salt” de 2 caracteres de ‘A’ até ‘M’ consecutivos, que poderiam aparecer no início ou final da palavra e misturada com uma versão da Enigma[[1]](#footnote-1) . Esta versão da Enigma consistia na troca de caracteres mediante a “plugboard” fornecida, um sistema de rotores, calculados em função do índex da letra(i), uma rotação(r) e um shift(s) ( i\*s+r).

# Desenvolvimento

Durante o desenvolvimento do programa, realizei duas versões do mesmo, a versão escolhida (A), e outra (B) que embora mais “eficiente” em termos de tempo, encontrava as palavras com o nosso R e/ou S diferentes. Tendo em conta que a verdadeira enigma funcionava mediante o fornecimento diário das configurações, para que todas as máquinas pudessem comunicar, optei pela versão A que obtém os resultados de R e S pretendidos.

A diferença entre as duas é que a versão B utiliza a palavra e ambos os “salts” para todo o processo, ou seja, tomemos como exemplo a palavra ANIMAS e o “salt” AS, na versão B teremos ‘ASANIMASAS’ a ir para a “plugboard”, “rotores” e “plugboard” novamente sendo separada em ‘ASANIMAS’ e ‘ANIMASAS’ apenas na fase de encriptação, isto faz com que nos rotores o índex das letras das palavras com “salt” no fim seja alterado, o que faz com que a palavra seja encontrada mas com configuração diferente. Optei então por uma forma hibrida (A) onde a palavra vai junta (ASNIMASAS) para os plugboards e é separada nos rotores e na encriptação. Isto é possível uma vez que as palavras possuem todas o mesmo tamanha, assim como o salt, por isso não é necessário separá-la nos plugboards, permitindo assim um aumento de performance.

# Programa

O programa roda com 3 argumentos, sendo o 1º a hash a encontrar, o 2º a plugboard e o 3º o txt como a lista de palavras a “correr”.

Caso não sejam introduzidos 3 rgumentos o programa avisa e encerra.

O algoritmo de Hash é calculado em função do tamanho da String introduzida como argumento 0. O programa verifica que a String apenas contém letras e numeros e depois mediante o tamanho aplica o algoritmo correspondente (128=SHA-512, 64=SHA-256, 32=SHA-128).

A plugboard terá que ser recebida no formato {char:char,char:char}, podendo os caracteres terem ou não pelicas. Só aceita letras como valores, no caso de ser introduzido um numero o programa avisa do erro e encerra, caso sejam inseridos 2 caracteres seguidos, apenas o primeiro é aceite e caso não seja inserido nada é ignorado.

Por fim o ficheiro com a lista de palavras terá que ser em formato txt e estar no dirétório do ficheiro java. Não é necessário indicar o caminho, mas se for tentado inserir outro caminho o programa encerra, caso seja tentado inserir algo como ./././wordlist.txt o programa automaticamente assume o dirétorio atual e ignora os ‘./’, neste caso se no dirétório atual houver um ficheiro wordlist.txt este é usado.

No final, ao encontrar a palavra, é possísel guardar os resultados em CSV (password, Posição do Salt, Salt, Rotação, Shift, algoritmo de hash e hash).

# BIBLIOGRAFIA

**AD DS**

Allen, R. (2021, January 02). How to add users to Active Directory Groups. Retrieved June 18, 2021, from https://activedirectorypro.com/add-users-to-active-directory-groups/

Dr Scripto Scripter, Scripto, D., 31, D., Scripto, D., & Villaronga, P. (2013, October 30). PowerTip: Create an Active Directory group with PowerShell. Retrieved June 18, 2021, from https://devblogs.microsoft.com/scripting/powertip-create-an-active-directory-group-with-powershell/

Francis, D., Saya, S., & Dor. (2018, October 07). Step-by-Step guide to INSTALL Active directory in Windows SERVER 2019 (PowerShell Guide) - technical blog. Retrieved June 18, 2021, from https://www.rebeladmin.com/2018/10/step-step-guide-install-active-directory-windows-server-2019-powershell-guide/

Hicks, J. (2016, February 03). Creating active Directory OUs with PowerShell. Retrieved June 18, 2021, from https://petri.com/creating-active-directory-ous-powershell

Jeff Melnick Jeff is a Director of Global Solutions Engineering at Netwrix. He is a long-time Netwrix blogger. (n.d.). How to create new Active Directory users with PowerShell. Retrieved June 18, 2021, from https://blog.netwrix.com/2018/06/07/how-to-create-new-active-directory-users-with-powershell/

**DNS SERVER**

Apply group policy to a security group. (2020, February 07). Retrieved June 18, 2021, from https://www.petenetlive.com/KB/Article/0001653

JasonGerend. (n.d.). Add-dnsserverforwarder (dnsserver). Retrieved June 18, 2021, from https://docs.microsoft.com/en-us/powershell/module/dnsserver/add-dnsserverforwarder?view=windowsserver2019-ps

Katie, & Ellis-Moore, L. (2020, March 25). Create & manage dns zones and records with PowerShell. Retrieved June 18, 2021, from <http://woshub.com/create-manage-dns-zones-records-powershell/>

**DHCP**

Dr Scripto Scripter, Scripto, D., 11, D., Scripto, D., & 12, D. (2013, January 11). Use PowerShell functions to Authorize DHCP Servers. Retrieved June 18, 2021, from https://devblogs.microsoft.com/scripting/use-powershell-functions-to-authorize-dhcp-servers/

How to install a dhcp server on Server Core | 4sysops. (n.d.). Retrieved June 18, 2021, from https://4sysops.com/archives/how-to-install-a-dhcp-server-on-server-core/

JasonGerend. (n.d.). Deploy dhcp using windows powershell. Retrieved June 18, 2021, from https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-deploy-wps

**RDS SERVER**

Bleeker, W. (2015, October 02). Convert pfx certificates to crt on windows. Retrieved June 18, 2021, from https://blog.wobl.it/2015/10/convert-pfx-certificates-to-crt-on-windows/

Deland-Han. (n.d.). Ferramentas de ADMINISTRAÇÃO DE Servidor REMOTO - Windows Server. Retrieved June 18, 2021, from https://docs.microsoft.com/pt-br/troubleshoot/windows-server/system-management-components/remote-server-administration-tools

JasonGerend. (n.d.). Features removed or planned for removal in windows server 2019. Retrieved June 18, 2021, from https://docs.microsoft.com/en-us/windows-server/get-started-19/removed-features-19

Jeff Melnick Jeff is a Director of Global Solutions Engineering at Netwrix. He is a long-time Netwrix blogger. (n.d.). How to automate powershell scripts with task scheduler. Retrieved June 18, 2021, from https://blog.netwrix.com/2018/07/03/how-to-automate-powershell-scripts-with-task-scheduler/

Lab: Implementing rds in windows server. (n.d.). Retrieved June 18, 2021, from https://microsoftlearning.github.io/WS-011-Windows-Server-2019-Administration/Instructions/Labs/LAB\_09\_Implementing\_RDS\_in\_Windows\_Server.html#exercise-3-configure-a-virtual-desktop-template

Powershell: Scheduled task with daily trigger and Repetition interval. Retrieved June 18, 2021, from https://stackoverflow.com/questions/20108886/powershell-scheduled-task-with-daily-trigger-and-repetition-interval

Step by step instructions for Installing RDS SESSION deployment using PowerShell in Windows Server 2012 R2. (2019, March 16). Retrieved June 18, 2021, from https://techcommunity.microsoft.com/t5/ask-the-performance-team/step-by-step-instructions-for-installing-rds-session-deployment/ba-p/375569

YongKW. (2021, January 24). Deploy Windows 2016 RDS with PowerShell. Retrieved June 18, 2021, from https://aventistech.com/2018/09/07/deploy-windows-2016-rds-with-powershell/

1. https://pt.wikipedia.org/wiki/Enigma\_(m%C3%A1quina) [↑](#footnote-ref-1)