NETWORK EXPLOITATION 101: MUITO ALÉM DO FIREWALL, UMA JORNADA DO DISCOVERY AO SHELL

Alexandro Silva
alexandro.silva@ibliss.digital

About.me

IBLISS DIGITAL SECURITY

- ✓ Diretor técnico na IBLISS Digital Security
- ✓ Professor
- ✓ Co-fundador da Nullbyte Security Conference

Objetivos

IBLISS DIGITAL SECURITY

- ✓ Fundamentos
- ✓ Mindset

Fundamentos

Fundamentos

IBLISS DIGITAL SECURITY

- ✓ Entedimento básico de:
  - ✓ Redes (topologia, ativos)
  - ✓ Protocolos
  - ✓ Serviços de rede (web, compatilhamento, email)

Mindset

Mindset

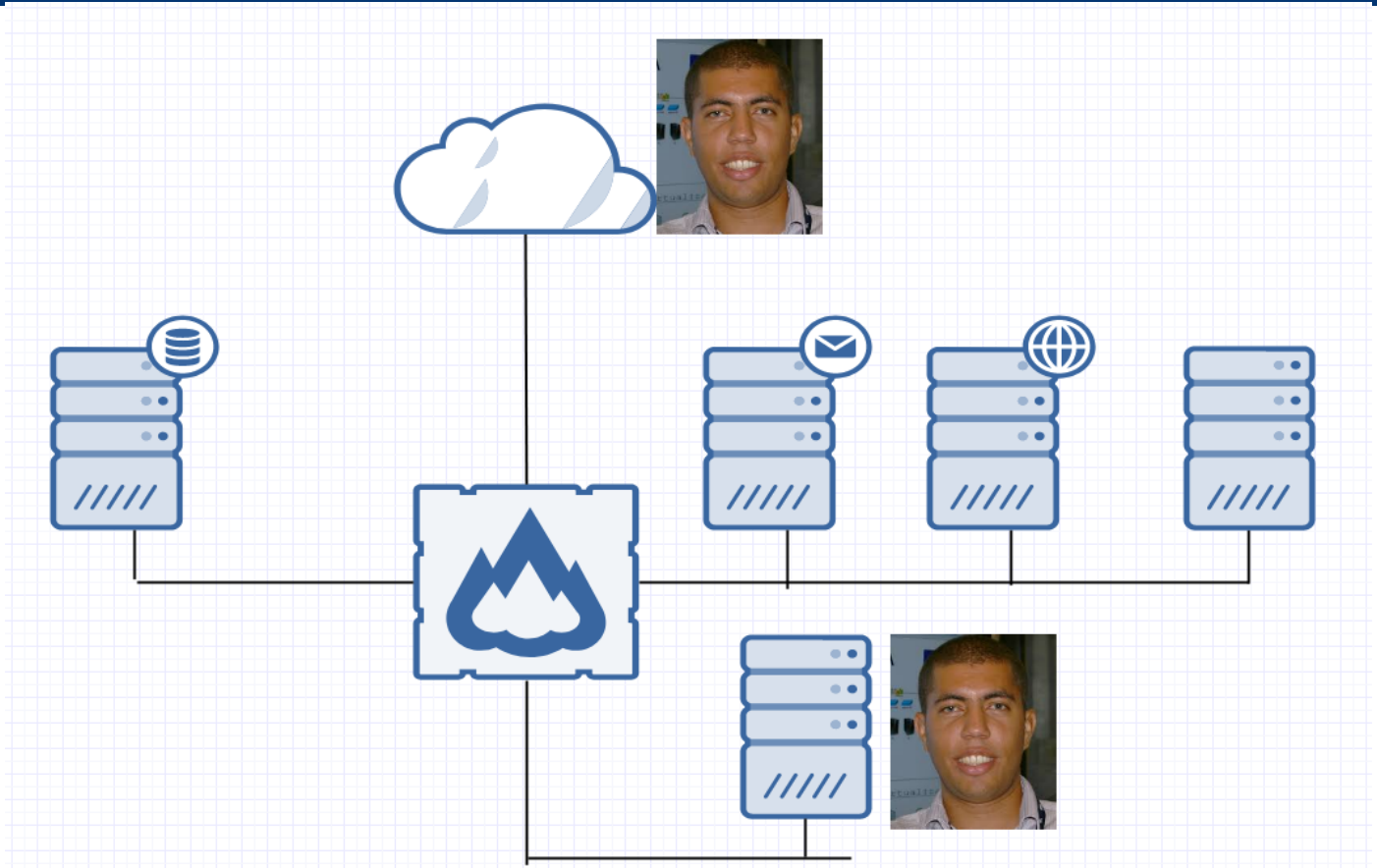
IBLISS DIGITAL SECURITY

- ✓ Enxergar além do óbvio;
- ✓ Se não existir uma ferramenta/ técnica, desenvolva ou aprimore o que existe;
- ✓ Pesquisar, Estudar e Entender.

Cenário

Cenário

IBLISS DIGITAL SECURITY



Metodologia

IBLISS DIGITAL SECURITY

Reconhecimento


LET'S HACK

Misconfigurantion


I
SMB

```
www.acme.com [192.168.11.13] 445 (microsoft-ds) open
smbd --version
Version 3.0.20-Debian
```

Samba "username map script" Command Execution

Disclosed	Created
05/14/2007	05/30/2018

Description

This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

SMB Exploitation

SMB Exploitation

IBLISS DIGITAL SECURITY

- ✓ Criar binário malicioso;
- ✓ Enviar para o servidor usando smbclient;
- ✓ Iniciar o listener;
- ✓ Executar o binário malicioso;
- ✓ Criar a persistência;
- ✓ Correr pro abraço!☺

Conclusão

IBLISS
DIGITAL SECURITY

contato@ibliss.digital

https://ibliss.digital

Portugal
Av. Casal Ribeiro, 28
Lisboa

+351 915 654 594

Brasil
Rua Nestor Pestana, 30 cj 156
São Paulo – SP

+55 11 3255-3926