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

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.

Lista de Imagens

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.

Histórico de Versionamento

Versão	Data	Autor	Descrição
1.0	01/04/1989	Bruno Botelho	*Versão Inicial.*

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.

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.

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.

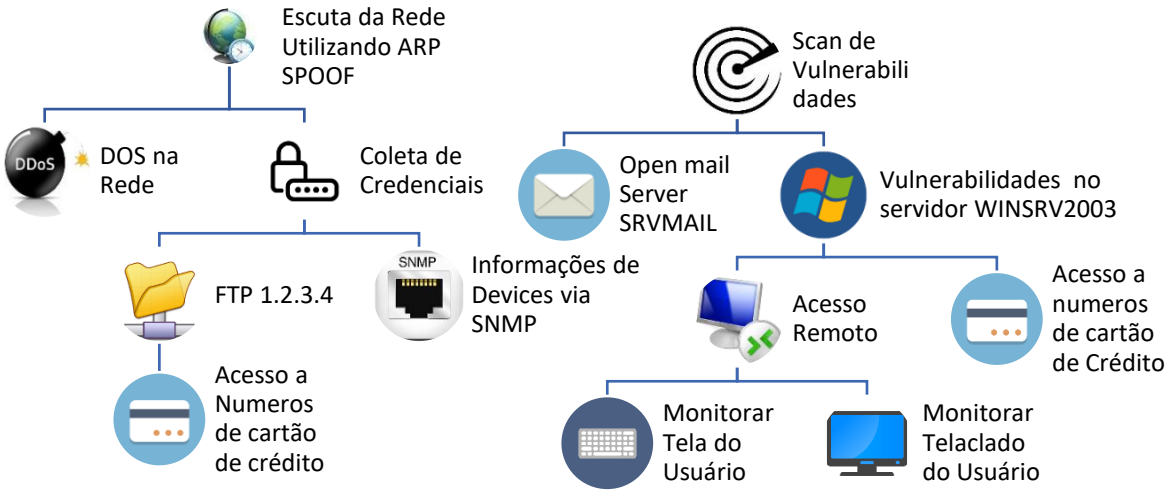
1 Sumário Executivo

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

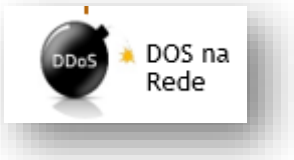
Objetivos alcançados:

- 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.



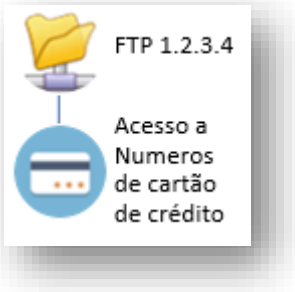
Inicialmente foi iniciado o processo de escuta na rede, a fim de ver tudo que passa na rede que esteja criptografado, a rede não tem controles que evitem o ataque de escuta de rede conhecido como “ARP SPOOF”, no plano de ação consta o que deve ser feito para inviabilizar ataques como este, como impacto,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



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.

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.

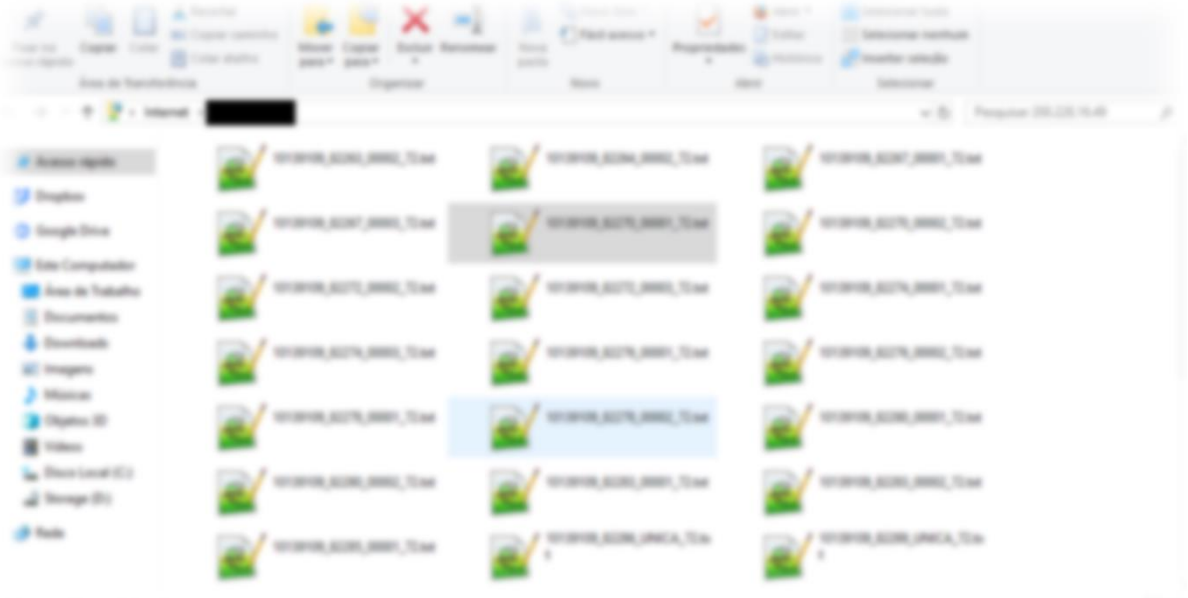


Figura 2 - Tela de Acesso ao servidor FTP do Banco XPTO

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.

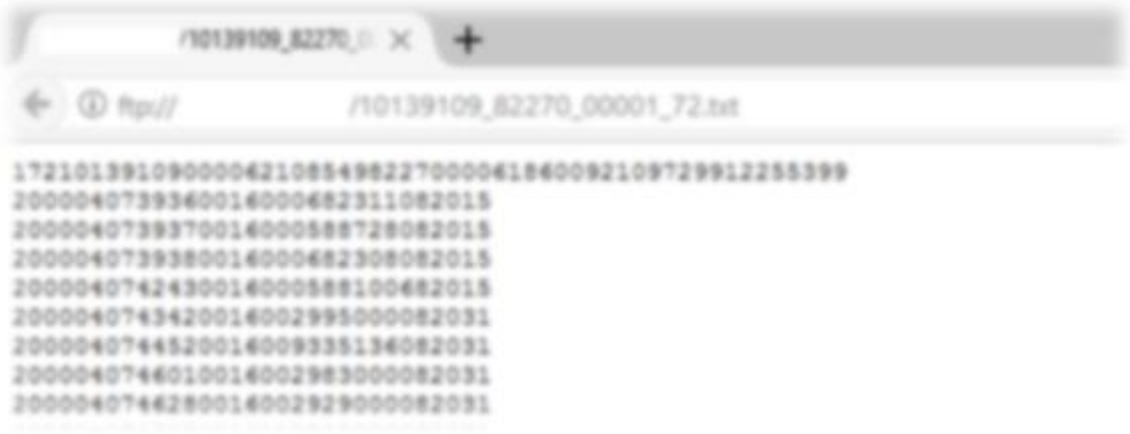
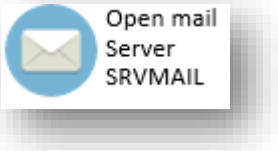


Figura 3 - Exemplo de arquivo com números de cartão de crédito contido no servidor do Banco XPTO

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.

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.

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 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.

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.

Figura 5 - Tela do Sistema que imprime cartões de crédito

```
eq";"NumRef";"Trilha1";"Trilha2";"Trilha3";"Trilha4";"Qtd"
0001";"JK5782800858BR";"6277801695700777=24106207091906901040";"";"";"";"1"
0002";"JK5782800948BR";"6277801695447064=24106202081906901040";"";"";"";"1"
0003";"JK5782801038BR";"6277801695361737=24106201531906901040";"";"";"";"1"
0004";"JK5782801178BR";"6277801695665772=24106202091906901040";"";"";"";"1"
0005";"JK5782801258BR";"6277801695714828=24106202311906901040";"";"";"";"1"
0006";"JK5782801348BR";"6277801694727136=24106200191906901040";"";"";"";"1"
0007";"JK5782801488BR";"6277801695095194=24106204981906901040";"";"";"";"1"
0008";"JK5782801518BR";"6277801695440168=24106205411906901040";"";"";"";"1"
0009";"JK5782801658BR";"6277801695854210=24106203451906901040";"";"";"";"1"
0010";"JK5782801798BR";"6277801695854269=24106207501906901040";"";"";"";"1"
0011";"JK5782801828BR";"6277801695854145=24106201501906901040";"";"";"";"1"
0012";"JK5782801968BR";"6277801695854277=24106209921906901040";"";"";"";"1"
0013";"JK5782802058BR";"6277801695854194=24106204051906901040";"";"";"";"1"
0014";"JK5782802198BR";"6277801695840037=24106209101906901040";"";"";"";"1"
0015";"JK5782802228BR";"6277801695854137=24106200451906901040";"";"";"";"1"
0016";"JK5782802368BR";"6277801695700884=24106207531906901040";"";"";"";"1"
0017";"JK5782802408BR";"6277801695359418=24106209041906901040";"";"";"";"1"
0018";"JK5782802538BR";"6277801695854020=24106203531906901040";"";"";"";"1"
0019";"JK5782802678BR";"6277801695307573=24106204221906901040";"";"";"";"1"
0020";"JK5782802758BR";"6277801695846844=24106202322906901040";"";"";"";"1"
0021";"JK5782802848BR";"6277801695361729=24106205191906901040";"";"";"";"1"
0022";"JK5782802988BR";"6277801695723068=24106206821906901040";"";"";"";"1"
0023";"JK5782803078BR";"6277801695679096=24106204211906901040";"";"";"";"1"
0024";"JK5782803158BR";"6277801695723159=24106203131906901040";"";"";"";"1"
0025";"JK5782803248BR";"6277801695463103=24106202521906901040";"";"";"";"1"
0026";"JK5782803388BR";"6277801695549398=24106206041906901040";"";"";"";"1"
0027";"JK5782803418BR";"6277801695203681=24106207831906901040";"";"";"";"1"
0028";"JK5782803558BR";"6277801695356224=24106206261906901040";"";"";"";"1"
0029";"JK5782803698BR";"6277801695307714=24106201411906901040";"";"";"";"1"
0030";"JK5782803728BR";"6277801695464457=24106201561906901040";"";"";"";"1"
0031";"JK5782803868BR";"6277801695850879=24106203051906901040";"";"";"";"1"
0032";"JK5782803908BR";"6277801695851018=24106205251906901040";"";"";"";"1"
0033";"JK5782804098BR";"6277801695307805=24106201251906901040";"";"";"";"1"
0034";"JK5782804128BR";"6277801695299325=24106209071906901040";"";"";"";"1"
0035";"JK5782804268BR";"6277801695307300=24106208231906901040";"";"";"";"1"
```

Figura 6 - Arquivos presentes no servidor para impressão

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.

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.

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.

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 nós a 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

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.

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

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.

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

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.

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.

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.

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.*

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.

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 expoits 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.

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.

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.

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. 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 administrator (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.

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.

4.2 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.

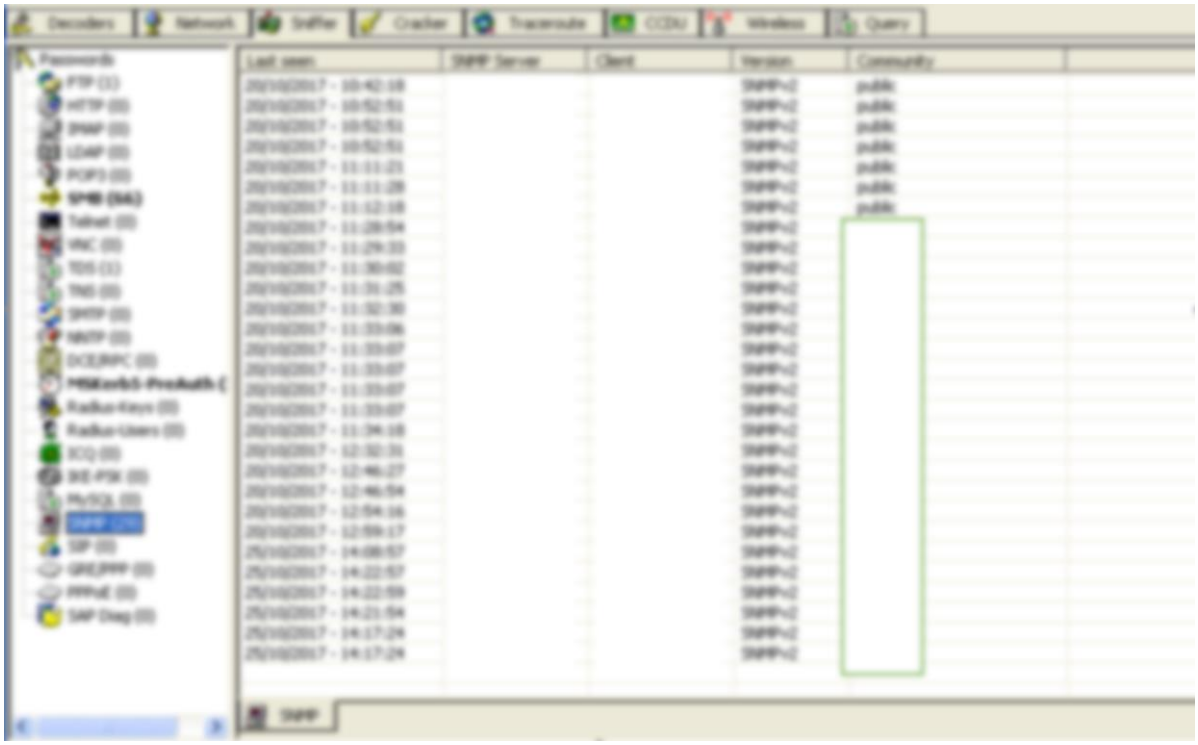
4.2.2 Sniffing de rede

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*

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.

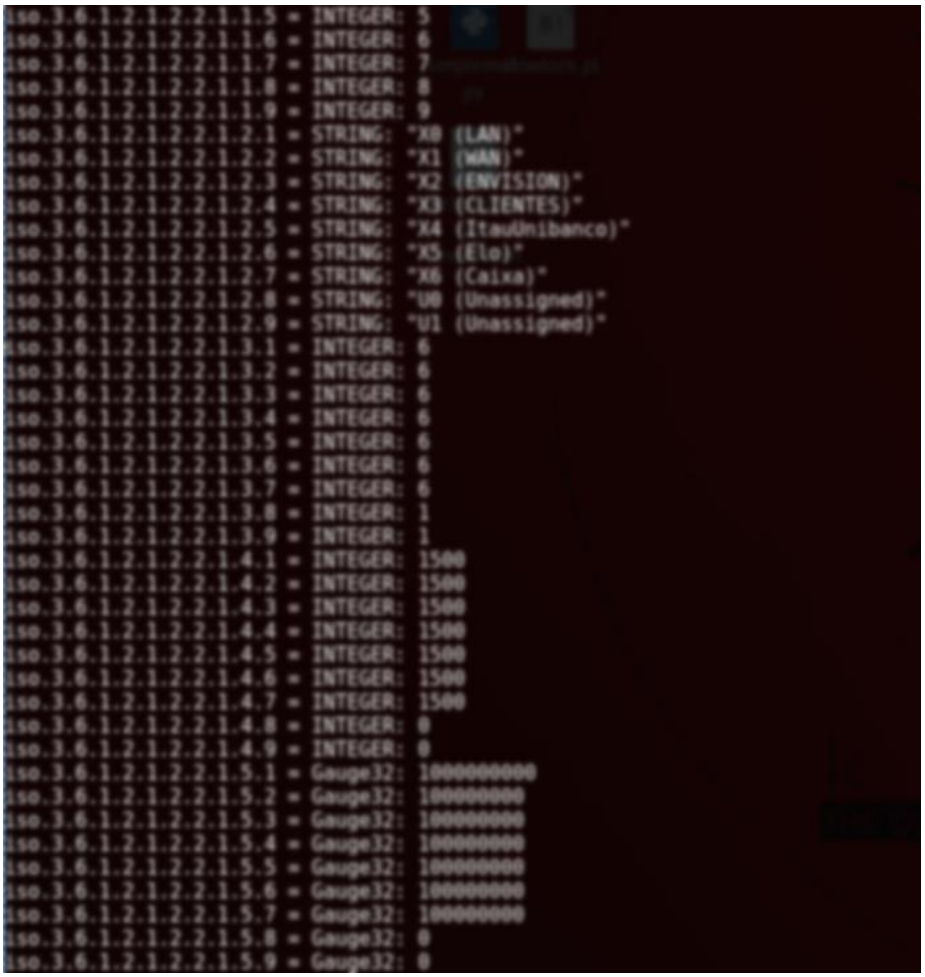


4.2.3 Acesso SNMP

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*

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.



4.2.4 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

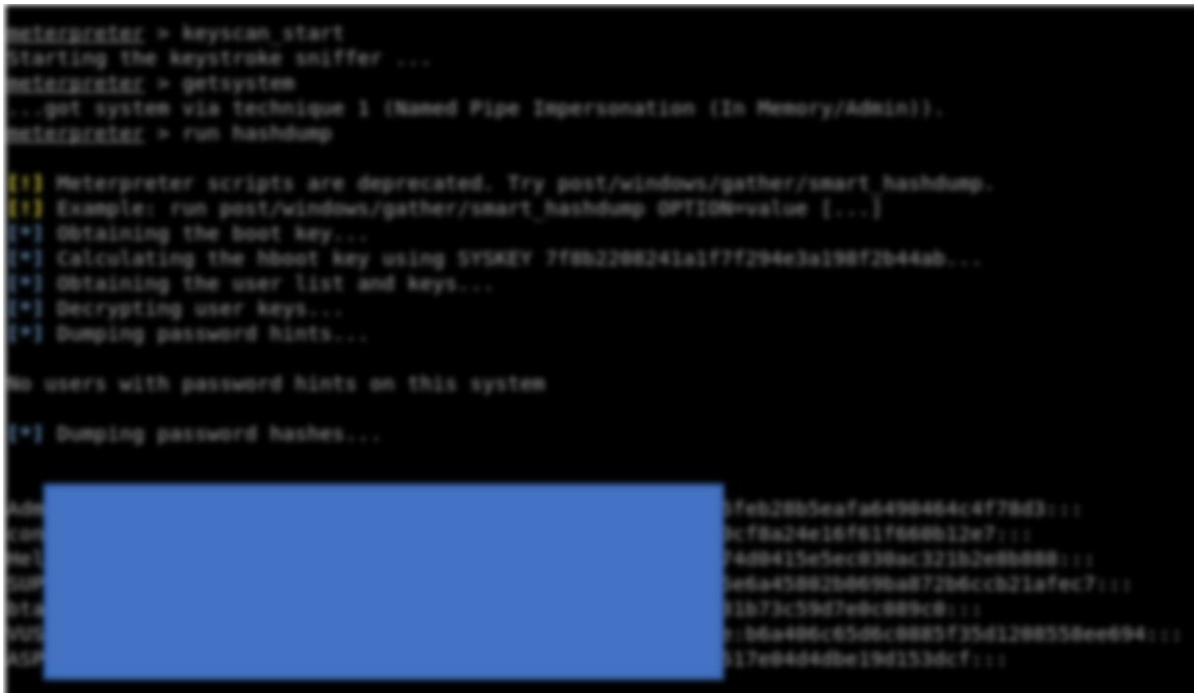
Foi resetada a senha do usuário administrador (Local) para Passw0rd.

Habilitamos remotamente o RDP na máquina.

Status - *Sucesso*

Evidências:

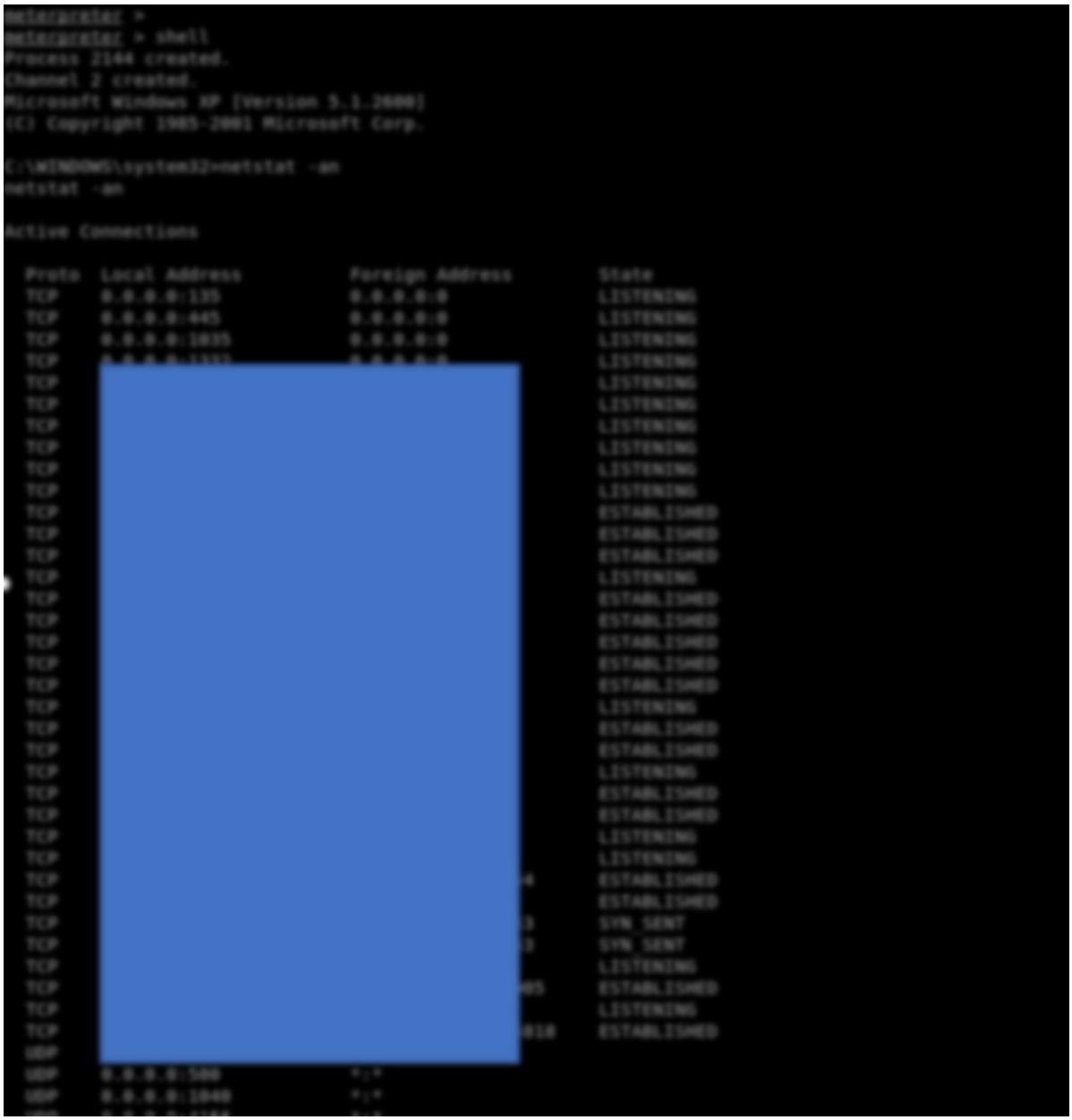
As informações contidas neste relatório são CONFIDENCIAIS e protegidas pelo sigilo legal. A divulgação, distribuição ou reprodução do teor deste documento depende de autorização da autorização do proprietário. Caso V. Sa. não seja o proprietário deste relatório, fica, desde já, notificado que qualquer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



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.

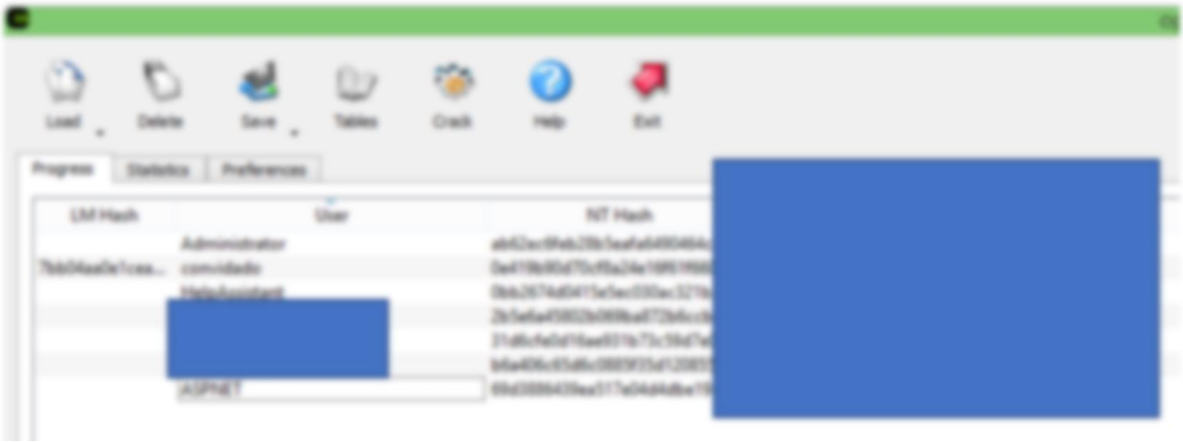
```
C:\WINDOWS\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Adm                                                                      btaw
con                                                                      UPPORT_388945a0
VUS
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.
```

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.

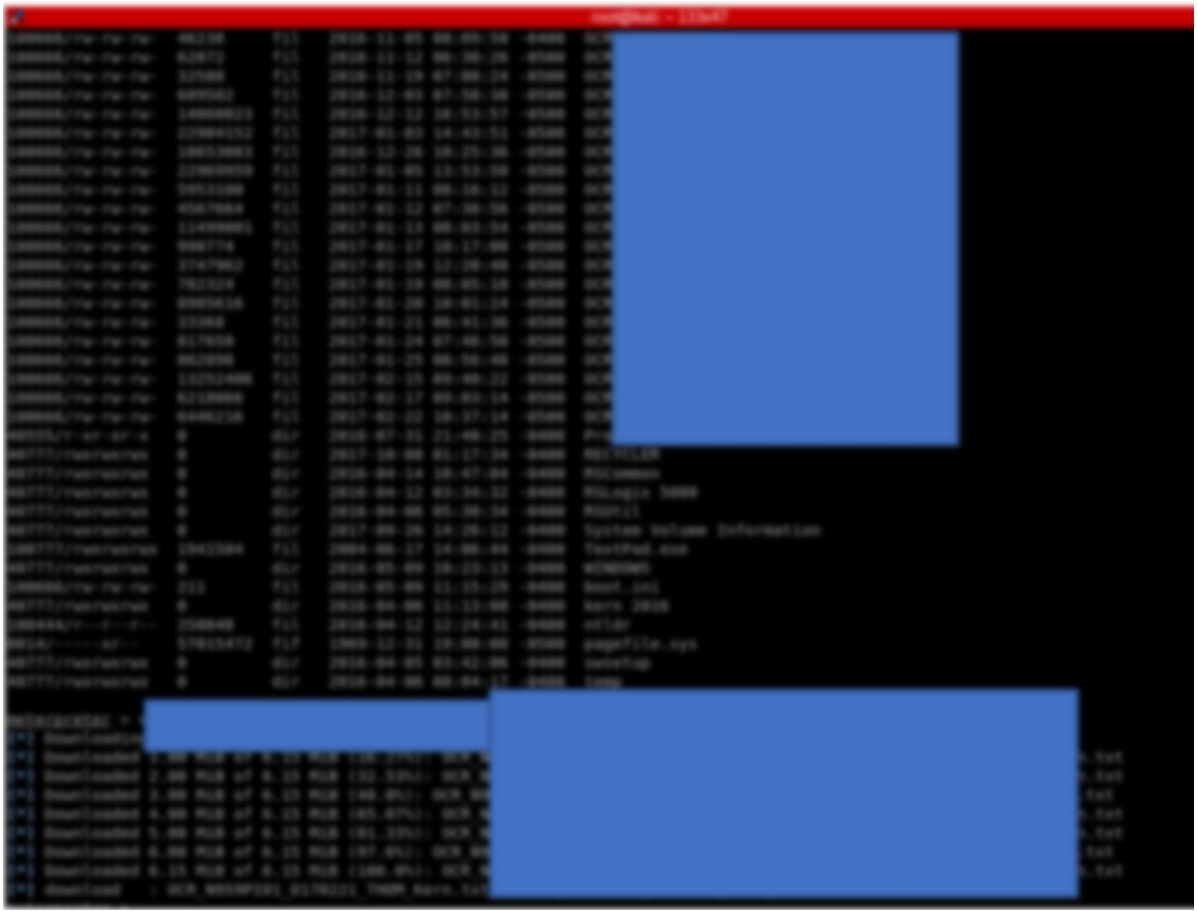


As informações contidas neste relatório são CONFIDENCIAIS e protegidas pelo sigilo legal. A divulgação, distribuição ou reprodução do teor deste documento depende de autorização da autorização do proprietário. Caso V. Sa. não seja o proprietário deste relatório, fica, desde já, notificado que qualquer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

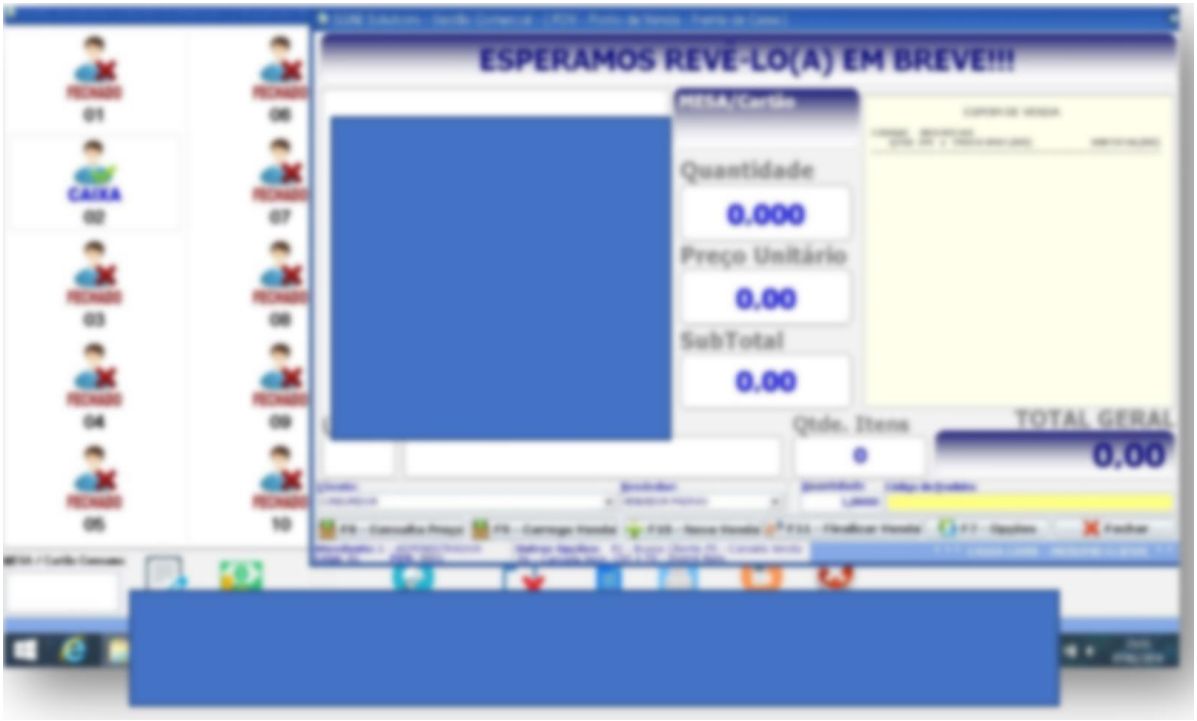
```
C:\WINDOWS\system32>net user Administrator
net user Administrator
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country code                 000 (System Default)
Account active               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 Passw0rd
net user Administrator Passw0rd
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 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.



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.



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.

4.2.5 Acesso ao FTP 1.2.3.4

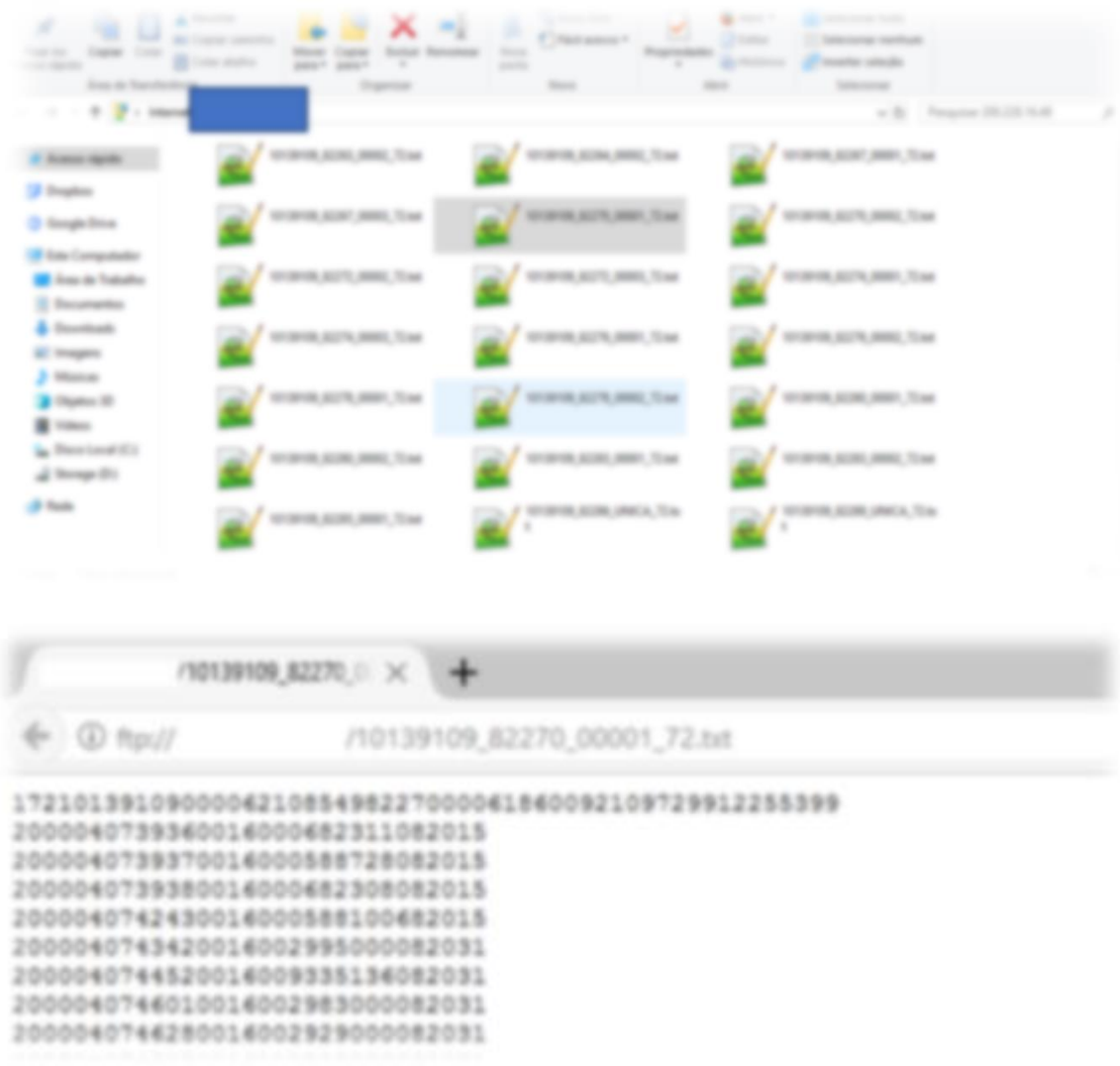
Utilizando a credenciais capturadas durante o ataque 1, tentamos acessar o FTP 1.2.3.4

Status *Sucesso*

Resultados Obtidos

Aparentemente há arquivos com números de cartões disponíveis neste FTP.

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.



4.2.6 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:

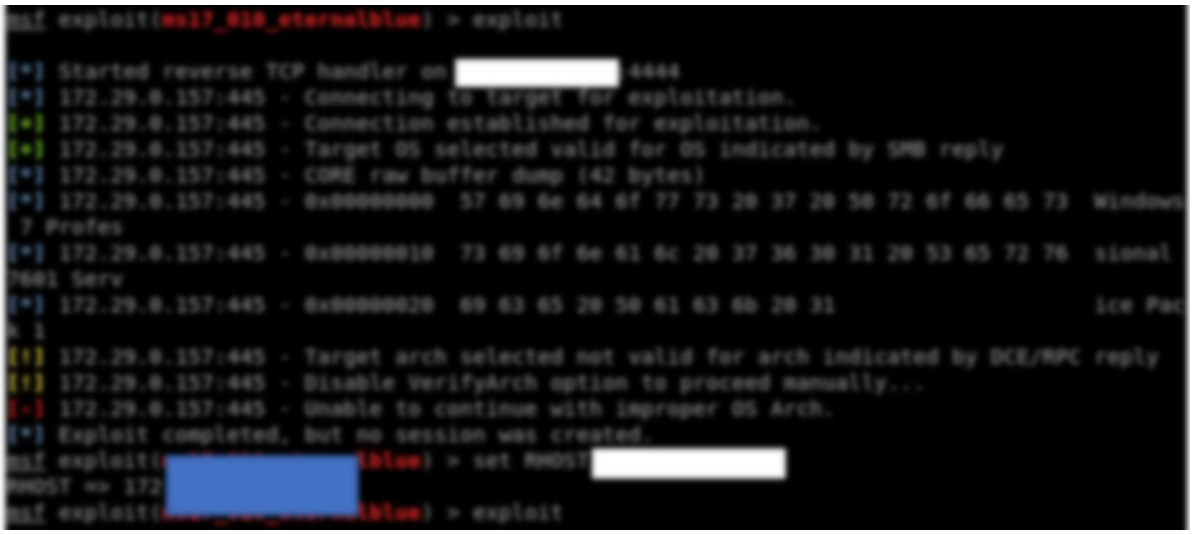
As informações contidas neste relatório são CONFIDENCIAIS e protegidas pelo sigilo legal. A divulgação, distribuição ou reprodução do teor deste documento depende de autorização da autorização do proprietário. Caso V. Sa. não seja o proprietário deste relatório, fica, desde já, notificado que qualquer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

4.2.7 Exploração da vulnerabilidade Etthernalblue (Wannacry)

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

Status - *Falha*

Evidências:



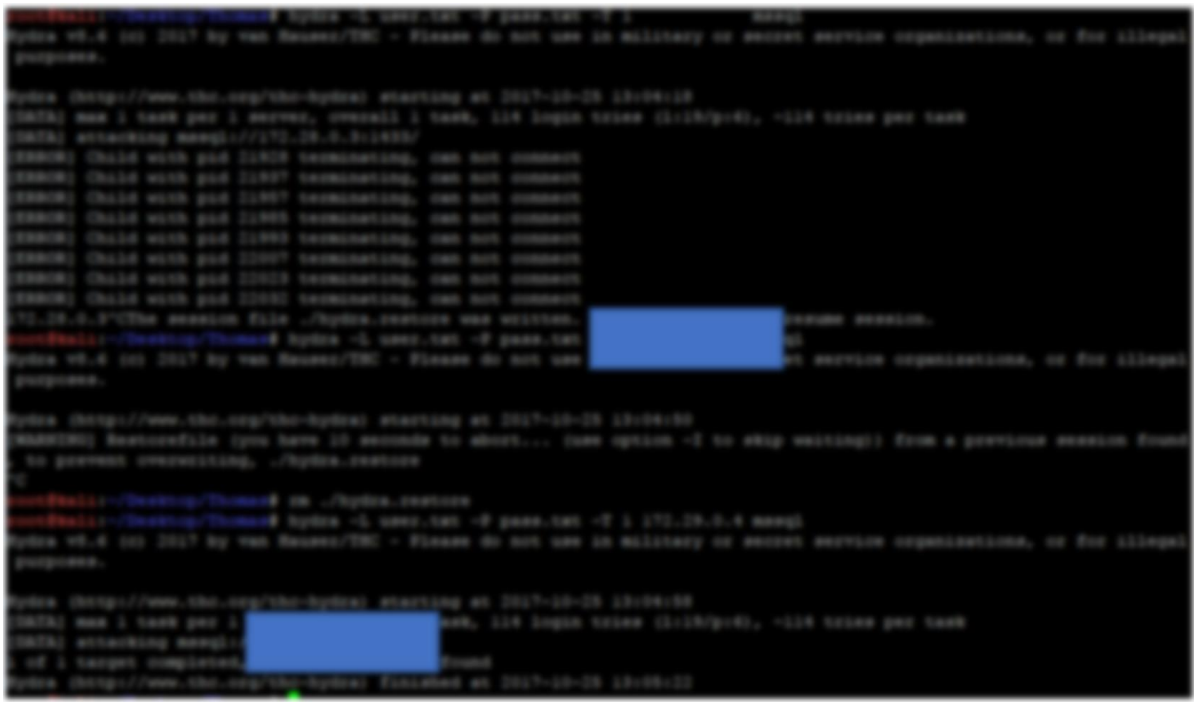
As informações contidas neste relatório são CONFIDENCIAIS e protegidas pelo sigilo legal. A divulgação, distribuição ou reprodução do teor deste documento depende de autorização da autorização do proprietário. Caso V. Sa. não seja o proprietário deste relatório, fica, desde já, notificado que qualquer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

4.2.8 Ataque de força bruta em servidores SQL

Tentamos acessar alguns servidores com um dicionário pequeno de usuários e senhas, não usamos um dicionário grande para não afetar a performance ou disponibilidade dos servidores.

Status - *Falha*

Evidências:



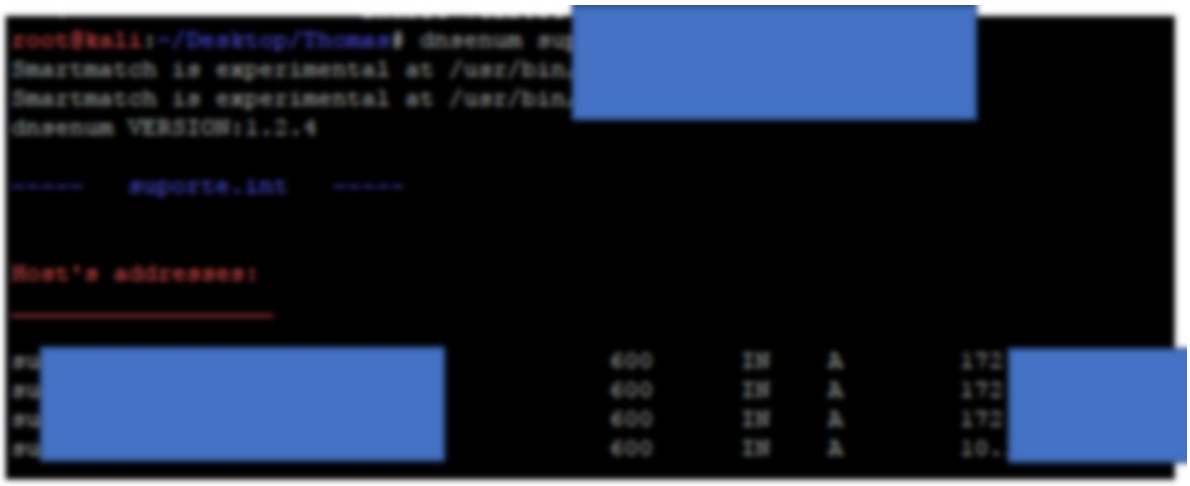
4.2.9 Ataque de transferência de Zona no DNS Interno

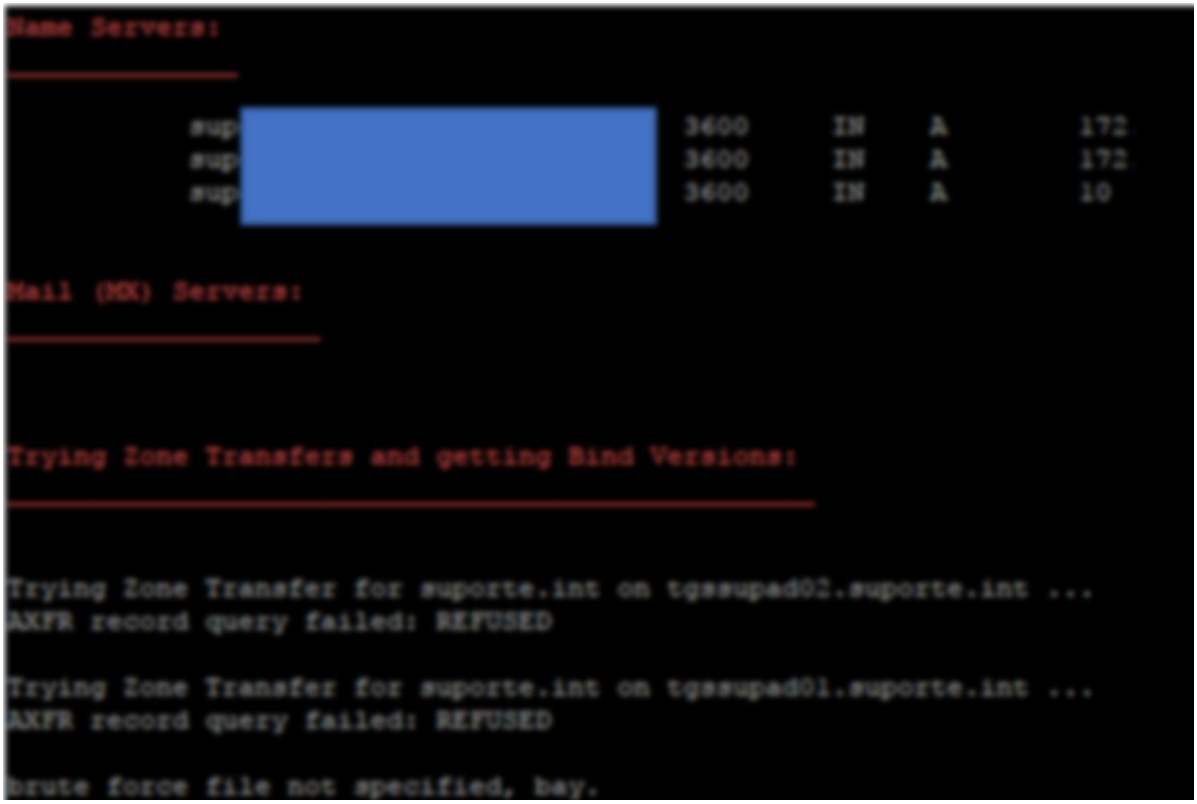
Tentativa de explorar algumas vulnerabilidades de configuração no DNS Interno.

Status - *Falha*

Evidências:

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.





4.2.10 Ataque de enumeração no servidor 9.8.7.6

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

Status - *Falha*

Evidências:

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.

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 ArpSopoof	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 comunity default "public" ou "private"	Sim

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.

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 dere, qualquer um pode imprimir documentos nelas.	Não

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.