OFFENSIVE SECURITY

Penetration Test Report for 10.0.0.82

Table of Contents

1.0 Comprehensive Network Discovery and Vulnerability Assessment Report for IP Address 10.0.0.82

1.1 Team Members

Natasha Siramarco
David Prutch
Raheem Reed
Dustin Haggett

1.1.1 Introduction

This Red Team Penetration Test Report outlines the comprehensive assessment undertaken as part of the project assigned by Simcorp to our team, "Binary Bandits 01." The assessment evaluates the security posture of Simcorp's network and systems through a series of controlled offensive security exercises on the specific IP address 10.0.0.82. The report emphasizes the accuracy, thoroughness, and technical proficiency required for successful penetration testing in alignment with Simcorp's security objectives. The primary goal is to demonstrate a deep understanding of penetration testing methodologies and technical expertise, supporting Simcorp's commitment to robust cybersecurity practices.

1.1.2 Objective

The primary objective of this assessment is to execute a rigorous internal penetration test on the specified target, IP address 10.0.0.82, as directed by our Red Team, Binary Bandits 01. Our team is responsible for adhering to a systematic methodology to gain access to this specific target, mirroring the processes involved in a real-world penetration test. This simulation aims to replicate the complexities of an actual penetration test on the target IP address, encompassing every stage from initiation to the comprehensive reporting phase. An example report template is available further in this document, serving as a valuable reference to assist our team in fulfilling the assessment requirements and achieving the desired outcomes for Simcorp's security evaluation.

1.1.3 Recommendations

Our assessment on IP address 10.0.0.82 highlights the critical importance of promptly addressing the identified vulnerabilities specific to this target. We strongly advise Simcorp to initiate a comprehensive patching process for this IP address to mitigate these vulnerabilities effectively. It is essential to recognize that this system necessitates regular and consistent patching. Ensuring that it remains on a recurring patch schedule is vital to safeguard against potential future vulnerabilities that may arise on IP address

10.0.0.82. By adhering to a proactive patch management approach for this specific target, Simcorp can significantly enhance its overall security posture.

1.1.4 Methodologies

Our approach to this assessment follows established and widely accepted penetration testing methodologies, which are proven to effectively evaluate the security posture of Simcorp's environment. The following section provides a comprehensive breakdown of the methodologies employed to assess the specific target, IP address 10.0.0.82, outlining the steps taken to identify and exploit various systems and documenting the specific vulnerabilities discovered during our assessment of this target.

2.0 Target Network

Binary Bandits 01 has conducted a comprehensive network scan of the target network, which encompasses the IP range 10.0.0.0/24. While our primary focus is on IP address 10.0.0.82, we have also included an overview of key findings and vulnerabilities within this broader network for context. The following table presents the results of our scan, highlighting notable findings and vulnerabilities across the network.

2.1 Scanned IP Address

IP Addresses Discovered	Protocols Discovered
10.0.0.82	21/tcp open ftp 80/tcp open http 135/tcp filtered msrpc 139/tcp filtered netbios-ssn 445/tcp filtered microsoft-ds 3389/tcp open ssl/ms-wbt-server? 49152/tcp open msrpc 49153/tcp open msrpc 49154/tcp open msrpc 49155/tcp open msrpc 49165/tcp open msrpc

3.0 Penetration

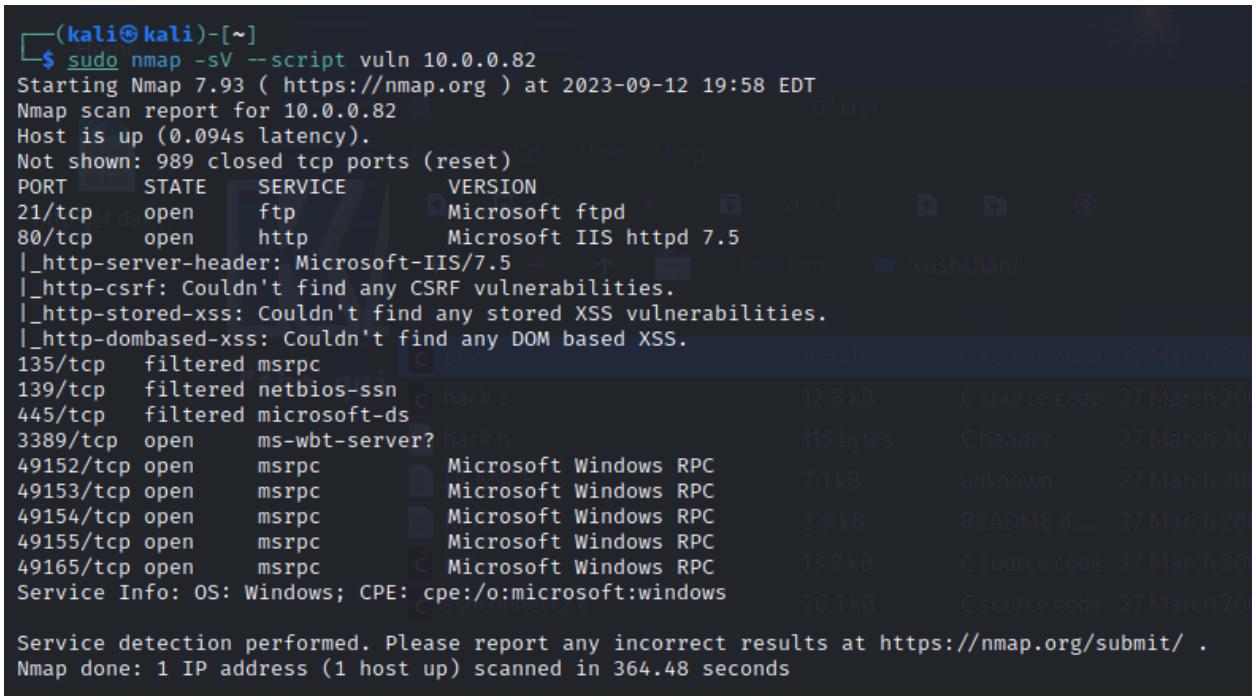
The penetration testing phase of our assessment is centered on gaining unauthorized access to the system at IP address 10.0.0.82. Throughout this penetration test, we successfully obtained access to this specific system within the IP range 10.0.0.0/24.

3.1 Service Enumeration

As part of our comprehensive penetration testing, we conducted service enumeration on the specified IP address 10.0.0.82. This critical phase involves collecting crucial information regarding the active services running on the target system. Such insights are invaluable to potential attackers, offering detailed knowledge about possible avenues for exploiting the system's vulnerabilities. Understanding the applications in operation is essential groundwork before proceeding with the actual penetration testing. It's worth noting that in certain cases, certain ports may not be listed as part of this enumeration process.

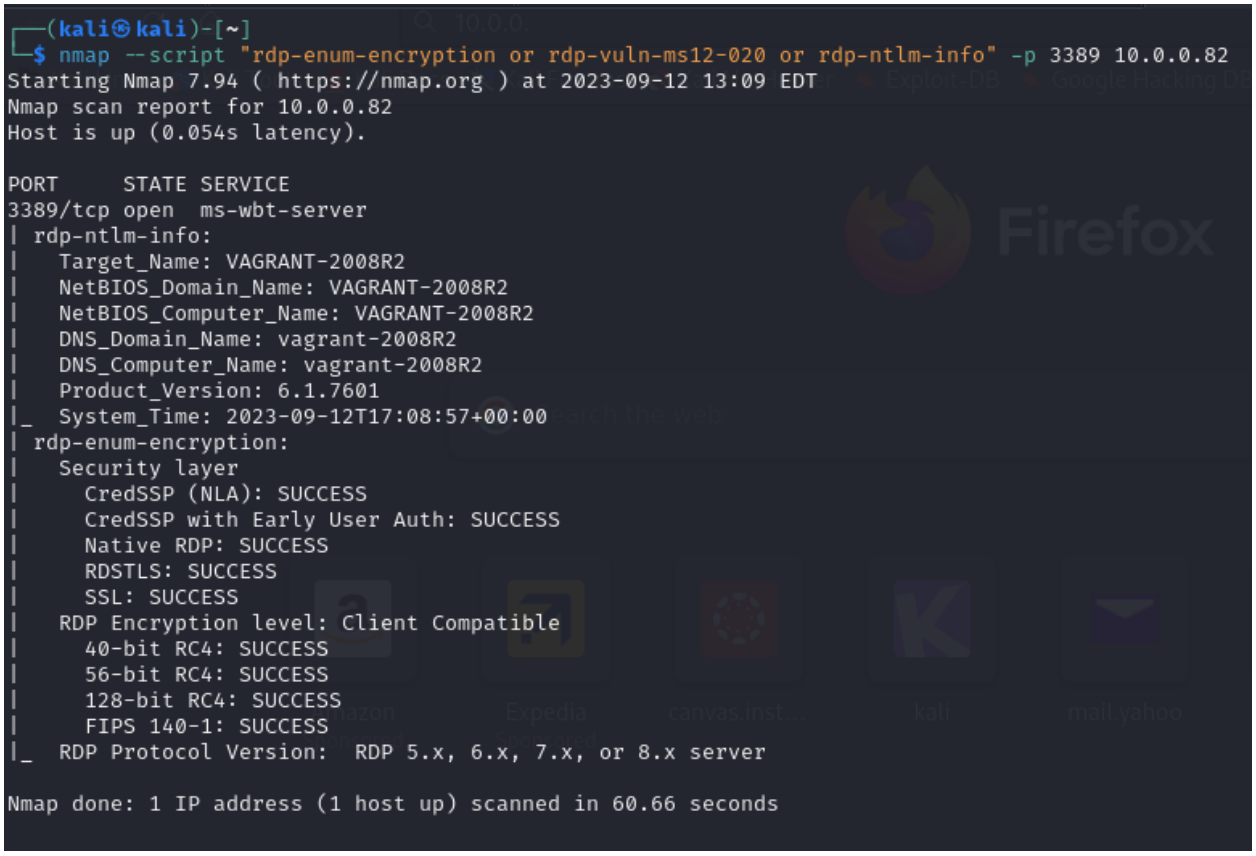
3.1 Vulnerability Assessment Report for IP Address 10.0.0.82

Vulnerability Scan



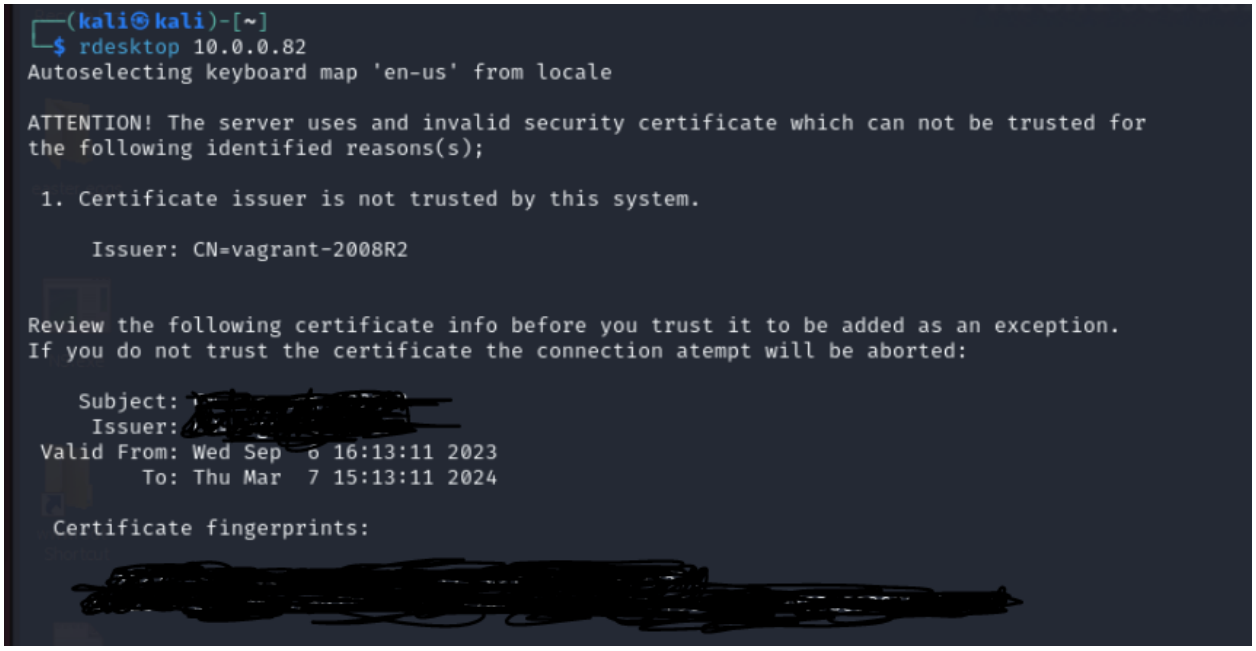
Enumeration Command:

nmap --script "rdp-enum-encryption or rdp-vuln-ms12-020 or rdp-ntlm-info" -p 3389 10.0.0.82

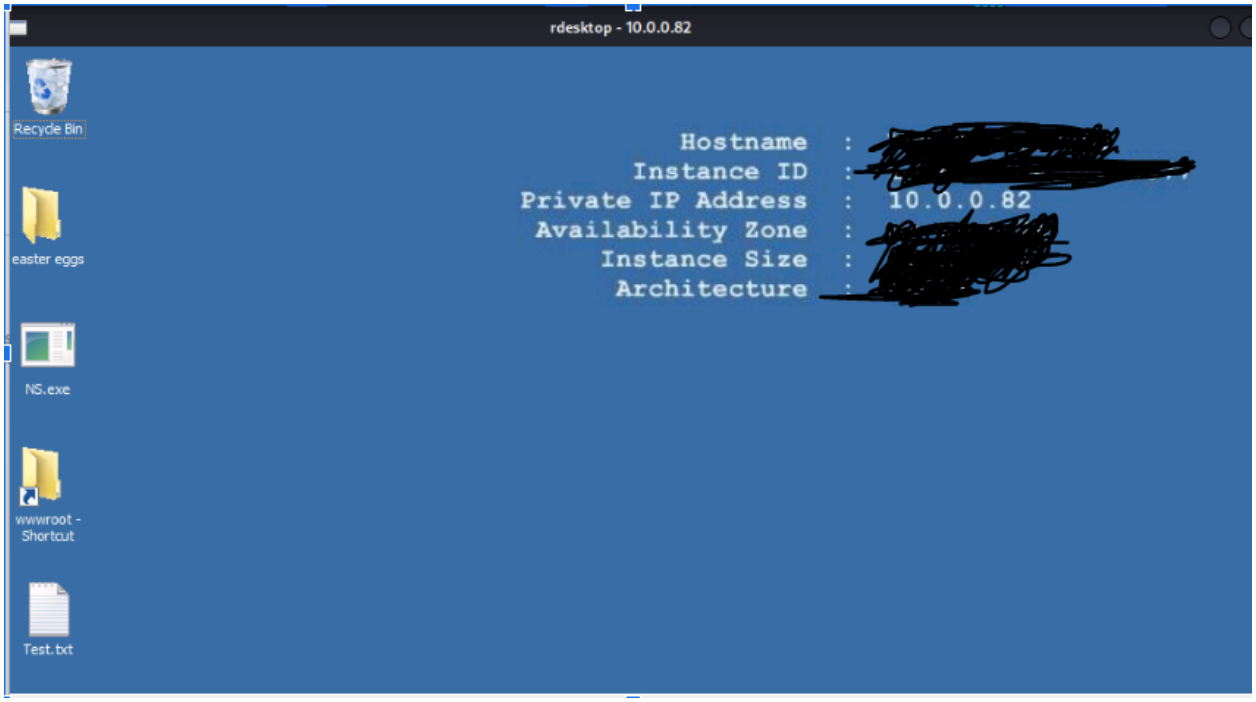


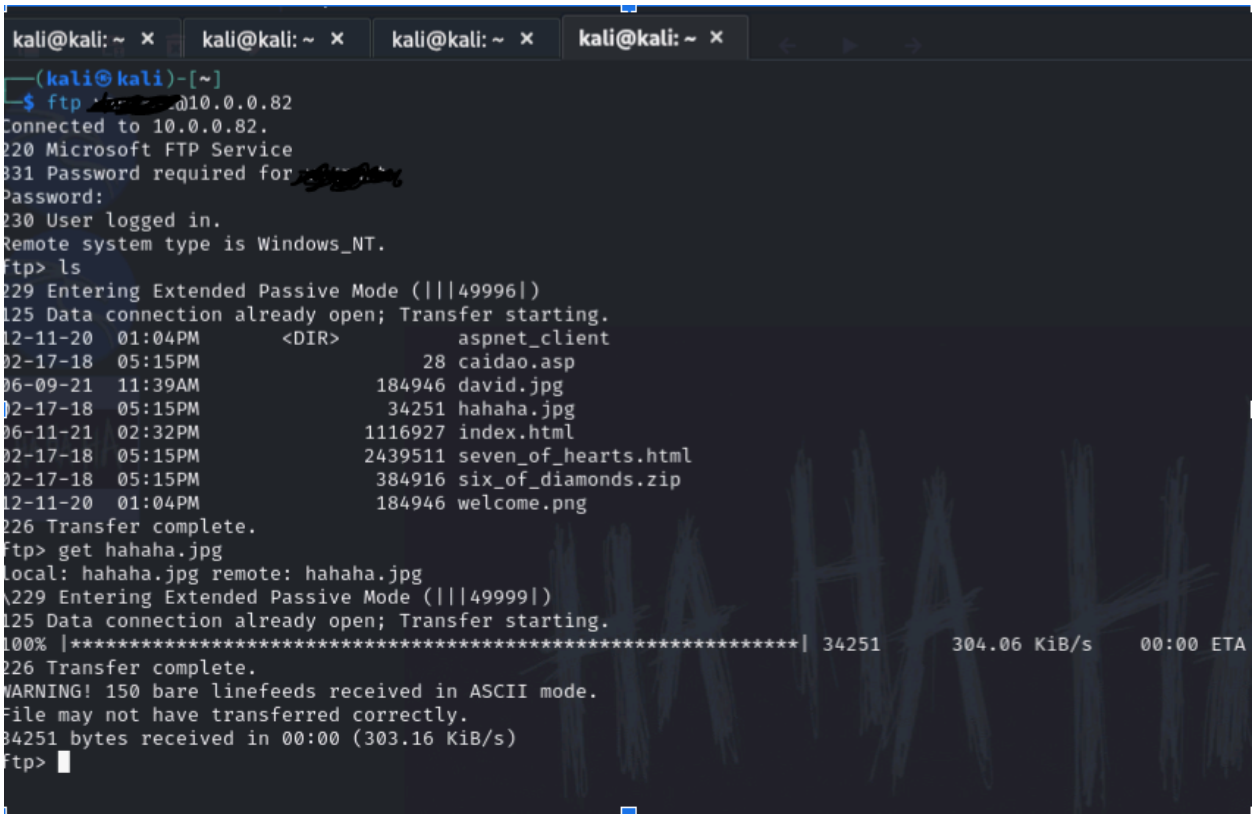
- Username: Has Been Identified
- Password: Has Been Identified

Remote Desktop

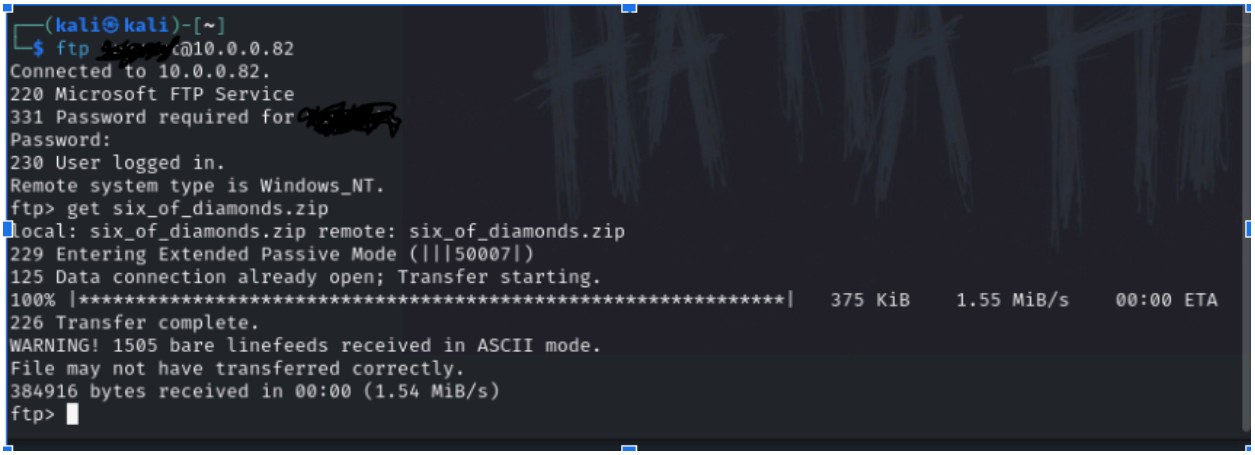



```
(kali㉿kali)-[~]
$ rdesktop 10.0.0.82
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
```

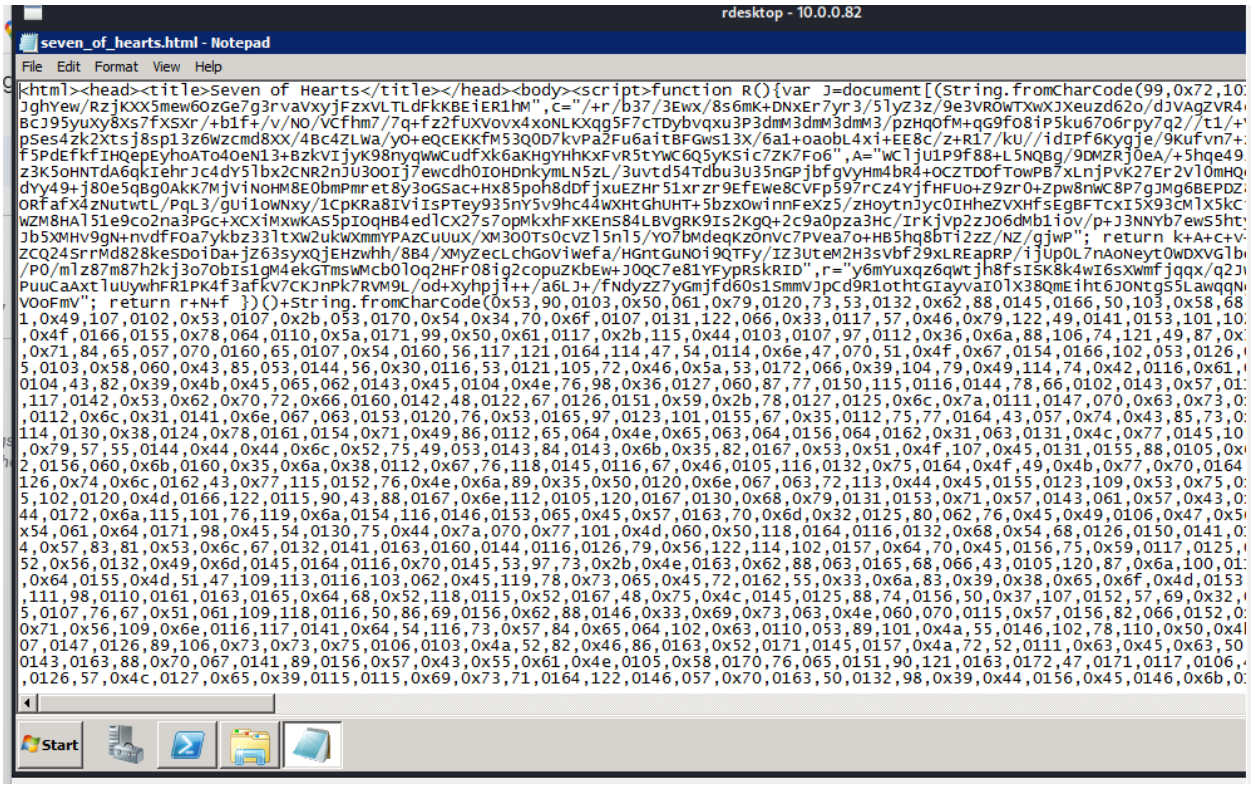

rdesktop - 10.0.0.82
Recycle Bin
easter eggs
NS.exe
wwwroot - Shortcut
Test.txt
Hostname :
Instance ID :
Private IP Address : 10.0.0.82
Availability Zone :
Instance Size :
Architecture :

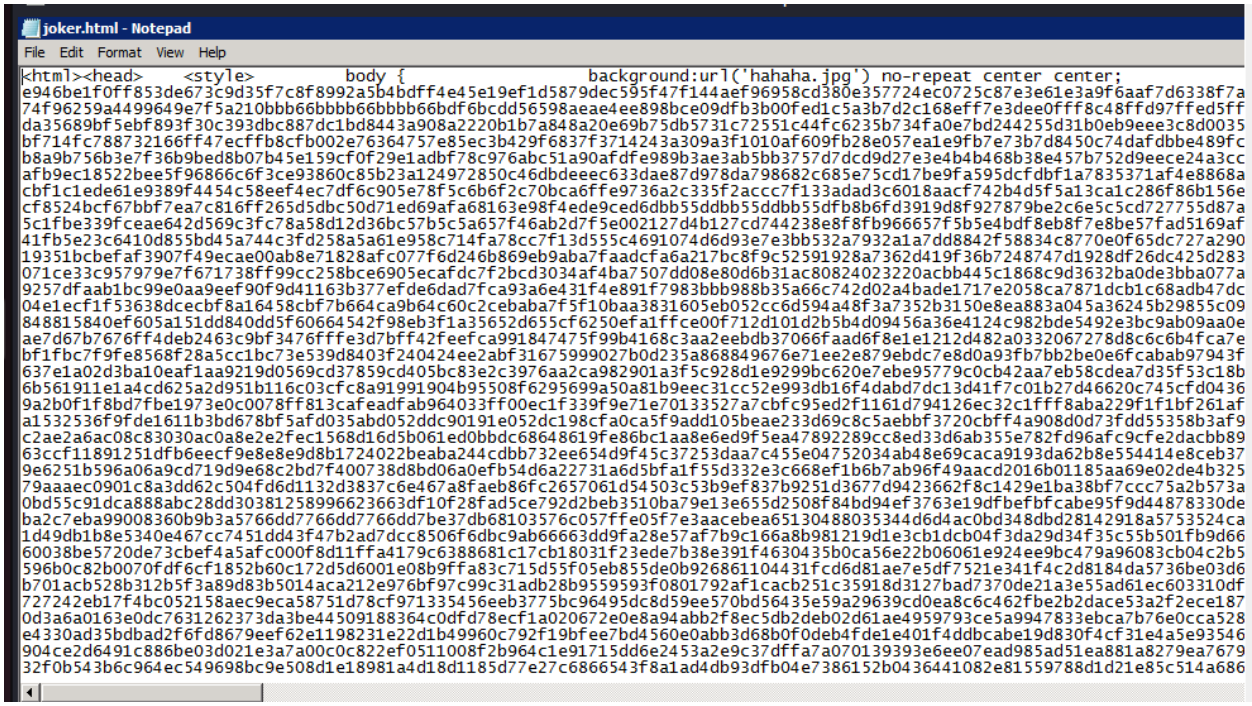

kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
(kali㉿kali)-[~]
$ ftp [redacted]@10.0.0.82
Connected to 10.0.0.82.
220 Microsoft FTP Service
331 Password required for [redacted]
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49996|)
125 Data connection already open; Transfer starting.
12-11-20 01:04PM <DIR> aspnet_client
02-17-18 05:15PM 28 caidao.asp
06-09-21 11:39AM 184946 david.jpg
02-17-18 05:15PM 34251 hahaha.jpg
06-11-21 02:32PM 1116927 index.html
02-17-18 05:15PM 2439511 seven_of_hearts.html
02-17-18 05:15PM 384916 six_of_diamonds.zip
12-11-20 01:04PM 184946 welcome.png
226 Transfer complete.
ftp> get hahaha.jpg
local: hahaha.jpg remote: hahaha.jpg
229 Entering Extended Passive Mode (|||49999|)
125 Data connection already open; Transfer starting.
100% |**********| 34251 304.06 KiB/s 00:00 ETA
226 Transfer complete.
WARNING! 150 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
34251 bytes received in 00:00 (303.16 KiB/s)
ftp>

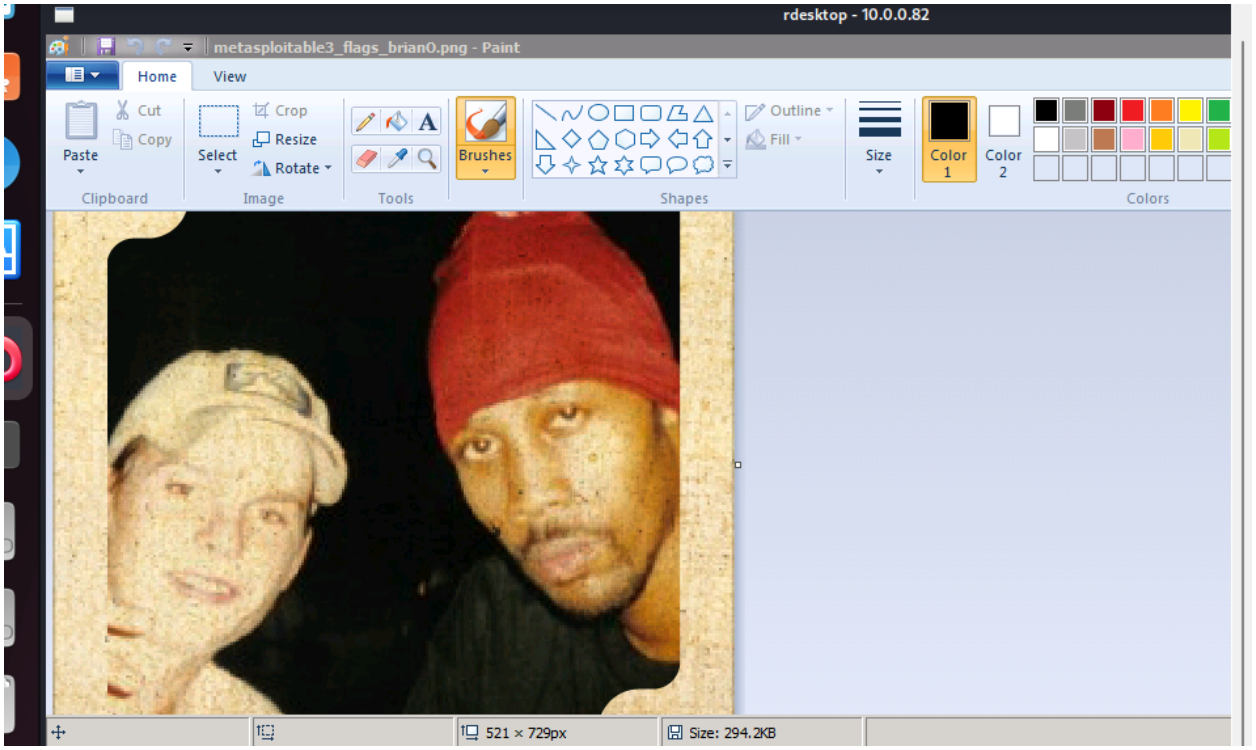
Get sixofdiamonds.zip

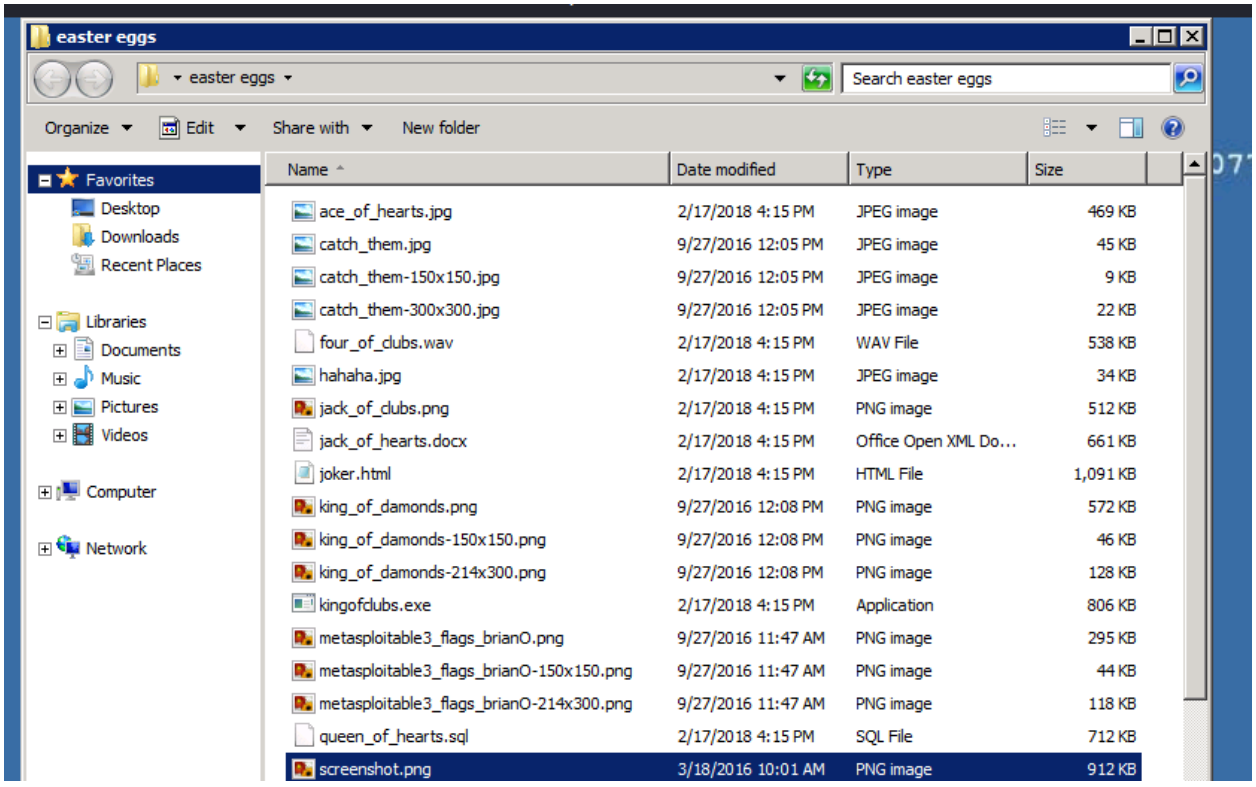


Easter Eggs

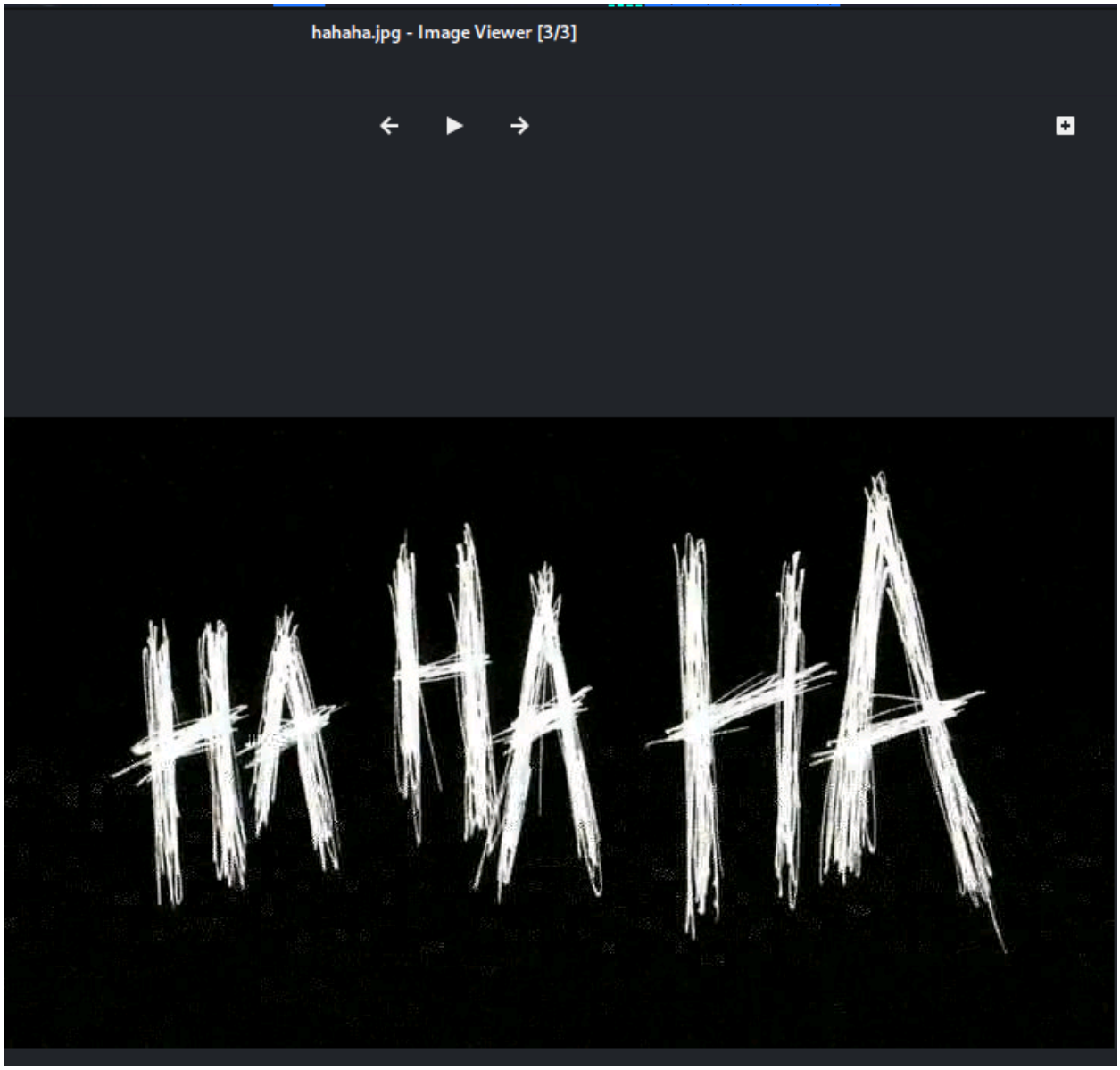



joker.html - Notepad
File Edit Format View Help
<html><head> <style> body { background:url('hahaha.jpg') no-repeat center center;
e946be1f0ff853de673c9d35f7c8f8992a5b4bdff4e45e19ef1d5879dec595f47f144aef96958cd380e357724ec0725c87e3e61e3a9f6aaf7d6338f7a
74f96259a4499649e7f5a210bbb66bbbb66bbbb66bdf6bcdd56598aeae4ee898bce09dfb3b00fed1c5a3b7d2c168eff7e3dee0fff8c48ffd97ffed5ff
da35689bf5ebf893f30c393dbc887dc1bd8443a908a2220b1b7a848a20e69b75db5731c72551c44fc6235b734fa0e7bd244255d31b0eb9eee3c8d0035
bf714fc788732166ff47ecffb8cfb002e76364757e85ec3b429f6837f3714243a309a3f1010af609fb28e057ea1e9fb7e73b7d8450c74dafdbbe489fc
b8a9b756b3e7f36b9bed8b07b45e159cf0f29e1adbf78c976abc51a90afdfe989b3ae3ab5bb3757d7dcd9d27e3e4b4b468b38e457b752d9eece24a3cc
afb9ec18522bee5f96866c6f3ce93860c85b23a124972850c46dbdeeec633dae87d978da798682c685e75cd17be9fa595dcfdbf1a7835371af4e8868a
cbf1c1ede61e9389f4454c58eef4ec7df6c905e78f5c6b6f2c70bca6ffe9736a2c335f2accc7f133adad3c6018aacf742b4d5f5a13ca1c286f86b156e
cf8524bcf67bbf7ea7c816ff265d5dbc50d71ed69afa68163e98f4ede9ced6dbb55ddbb55ddbb55dfb8b6fd3919d8f927879be2c6e5c5cd727755d87a
5c1fbe339fceae642d569c3fc78a58d12d36bc57b5c5a657f46ab2d7f5e002127d4b127cd744238e8f8fb966657f5b5e4bdf8eb8f7e8be57fad5169af
41fb5e23c6410d855bd45a744c3fd258a5a61e958c714fa78cc7f13d555c4691074d6d93e7e3bb532a7932a1a7dd8842f58834c8770e0f65dc727a290
19351bcbefaf3907f49ecae00ab8e71828afc077f6d246b869eb9aba7faadcfa6a217bc8f9c52591928a7362d419f36b7248747d1928df26dc425d283
071ce33c957979e7f671738ff99cc258bce6905ecafdc7f2bcd3034af4ba7507dd08e80d6b31ac80824023220acbb445c1868c9d3632ba0de3bba077a
9257dfaab1bc99e0aa9eef90f9d41163b377efde6dad7fca93a6e431f4e891f7983bbb988b35a66c742d02a4bade1717e2058ca7871dcb1c68adb47dc
04e1ecf1f53638dcecbf8a16458cbf7b664ca9b64c60c2cebaba7f5f10baa3831605eb052cc6d594a48f3a7352b3150e8ea883a045a36245b29855c09
848815840ef605a151dd840dd5f60664542f98eb3f1a35652d655cf6250efa1ffce00f712d101d2b5b4d09456a36e4124c982bde5492e3bc9ab09aa0e
ae7d67b7676ff4deb2463c9bf3476fffe3d7bff42feefca991847475f99b4168c3aa2eebdb37066faad6f8e1e1212d482a0332067278d8c6c6b4fca7e
bf1fbc7f9fe8568f28a5cc1bc73e539d8403f240424ee2abf31675999027b0d235a868849676e71ee2e879ebdc7e8d0a93fb7bb2be0e6fcabab97943f
637e1a02d3ba10eaf1aa9219d0569cd37859cd405bc83e2c3976aa2ca982901a3f5c928d1e9299bc620e7ebe95779c0cb42aa7eb58cdea7d35f53c18b
6b561911e1a4cd625a2d951b116c03cfc8a91991904b95508f6295699a50a81b9eec31cc52e993db16f4dabd7dc13d41f7c01b27d46620c745cfd0436
9a2b0f1f8bd7fbe1973e0c0078ff813cafeadfab964033ff00ec1f339f9e71e70133527a7cbfc95ed2f1161d794126ec32c1fff8aba229f1f1bf261af
a1532536f9fde1611b3bd678bf5afd035abd052ddc90191e052dc198cfa0ca5f9add105beae233d69c8c5aebbf3720cbff4a908d0d73fdd55358b3af9
c2ae2a6ac08c83030ac0a8e2e2fec1568d16d5b061ed0bbdc68648619fe86bc1aa8e6ed9f5ea47892289cc8ed33d6ab355e782fd96afc9cfe2dacbb89
63ccf11891251dfb6eecf9e8e8e9d8b1724022beaba244cdbb732ee654d9f45c37253daa7c455e04752034ab48e69caca9193da62b8e554414e8ceb37
9e6251b596a06a9cd719d9e68c2bd7f400738d8bd06a0efb54d6a22731a6d5bfa1f55d332e3c668ef1b6b7ab96f49aacd2016b01185aa69e02de4b325
79aaaec0901c8a3dd62c504fd6d1132d3837c6e467a8faeb86fc2657061d54503c53b9ef837b9251d3677d9423662f8c1429e1ba38bf7ccc75a2b573a
0bd55c91dca888abc28dd3038125899662366 3df10f28fad5ce792d2beb3510ba79e13e655d2508f84bd94ef3763e19dfbefbfcabe95f9d44878330de
ba2c7eba99008360b9b3a5766dd7766dd7766dd7be37db68103576c057ffe05f7e3aacebea65130488035344d6d4ac0bd348dbd28142918a5753524ca
1d49db1b8e5340e467cc7451dd43f47b2ad7dcc8506f6dbc9ab66663dd9fa28e57af7b9c166a8b981219d1e3cb1dcb04f3da29d34f35c55b501fb9d66
60038be5720de73cbef4a5afc000f8d11ffa4179c6388681c17cb18031f23ede7b38e391f4630435b0ca56e22b06061e924ee9bc479a96083cb04c2b5
596b0c82b0070fdf6cf1852b60c172d5d6001e08b9ffa83c715d55f05eb855de0b926861104431fcd6d81ae7e5df7521e341f4c2d8184da5736be03d6
b701acb528b312b5f3a89d83b5014aca212e976bf97c99c31adb28b9559593f0801792af1cacb251c35918d3127bad7370de21a3e55ad61ec603310df
727242eb17f4bc052158aec9eca58751d78cf971335456eeb3775bc96495dc8d59ee570bd56435e59a29639cd0ea8c6c462fbe2b2dace53a2f2ece187
0d3a6a0163e0dc7631262373da3be44509188364c0dfd78ecf1a020672e0e8a94abb2f8ec5db2deb02d61ae4959793ce5a9947833ebca7b76e0cca528
e4330ad35bdbad2f6fd8679eef62e1198231e22d1b49960c792f19bfee7bd4560e0abb3d68b0f0deb4fde1e401f4ddbcabe19d830f4cf31e4a5e93546
904ce2d6491c886be03d021e3a7a00c0c822ef0511008f2b964c1e91715dd6e2453a2e9c37dffa7a070139393e6ee07ead985ad51ea881a8279ea7679
32f0b543b6c964ec549698bc9e508d1e18981a4d18d1185d77e27c6866543f8a1ad4db93dfb04e7386152b0436441082e81559788d1d21e85c514a686

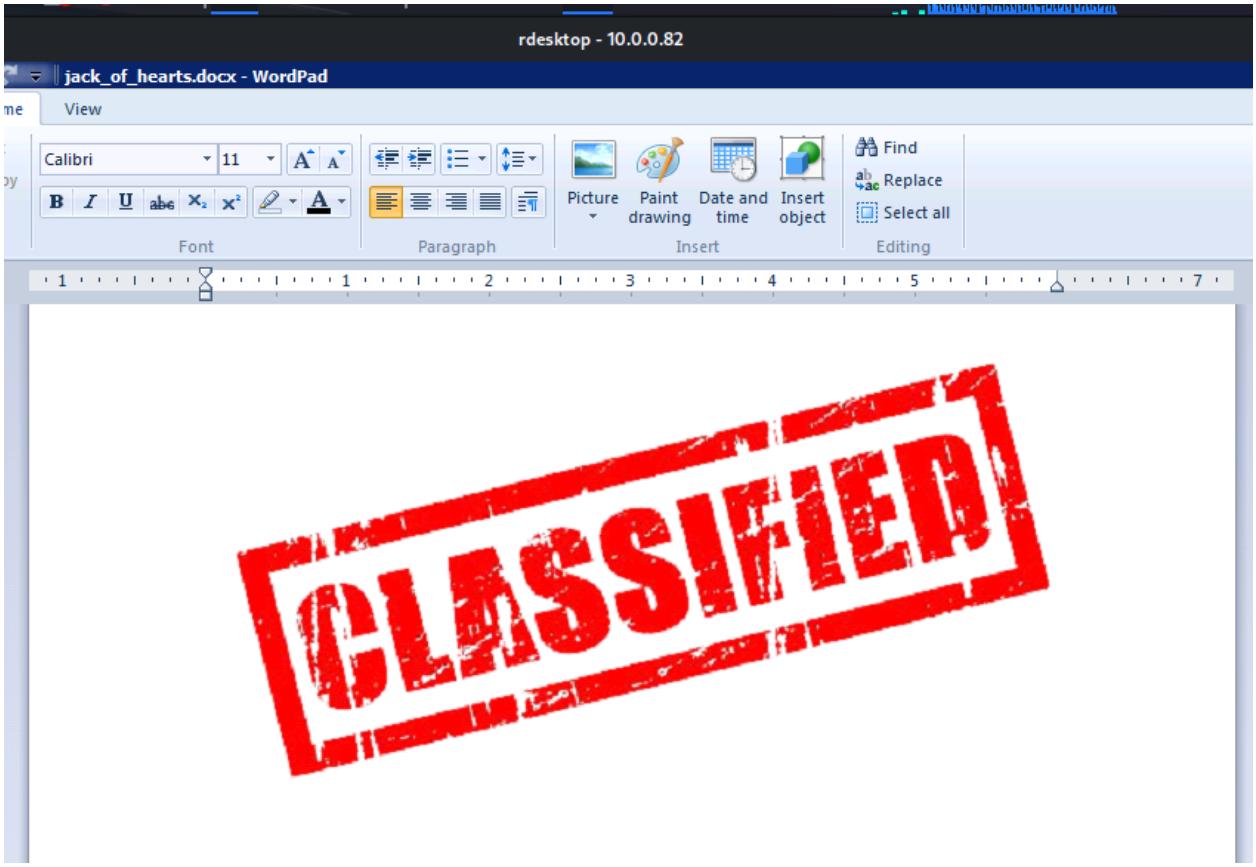

rdesktop - 10.0.0.82
metasploitable3_flags_brianO.png - Paint
Home
View
Paste
Cut
Copy
Select
Crop
Resize
Rotate
Brushes
Outline
Fill
Size
Color 1
Color 2
Clipboard
Image
Tools
Shapes
Colors
521 × 729px
Size: 294.2KB


easter eggs
Search easter eggs
Organize
Edit
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
ace_of_hearts.jpg 2/17/2018 4:15 PM JPEG image 469 KB
catch_them.jpg 9/27/2016 12:05 PM JPEG image 45 KB
catch_them-150x150.jpg 9/27/2016 12:05 PM JPEG image 9 KB
catch_them-300x300.jpg 9/27/2016 12:05 PM JPEG image 22 KB
four_of_clubs.wav 2/17/2018 4:15 PM WAV File 538 KB
hahaha.jpg 2/17/2018 4:15 PM JPEG image 34 KB
jack_of_clubs.png 2/17/2018 4:15 PM PNG image 512 KB
jack_of_hearts.docx 2/17/2018 4:15 PM Office Open XML Do... 661 KB
joker.html 2/17/2018 4:15 PM HTML File 1,091 KB
king_of_damonds.png 9/27/2016 12:08 PM PNG image 572 KB
king_of_damonds-150x150.png 9/27/2016 12:08 PM PNG image 46 KB
king_of_damonds-214x300.png 9/27/2016 12:08 PM PNG image 128 KB
kingofclubs.exe 2/17/2018 4:15 PM Application 806 KB
metasploitable3_flags_brianO.png 9/27/2016 11:47 AM PNG image 295 KB
metasploitable3_flags_brianO-150x150.png 9/27/2016 11:47 AM PNG image 44 KB
metasploitable3_flags_brianO-214x300.png 9/27/2016 11:47 AM PNG image 118 KB
queen_of_hearts.sql 2/17/2018 4:15 PM SQL File 712 KB
screenshot.png 3/18/2016 10:01 AM PNG image 912 KB

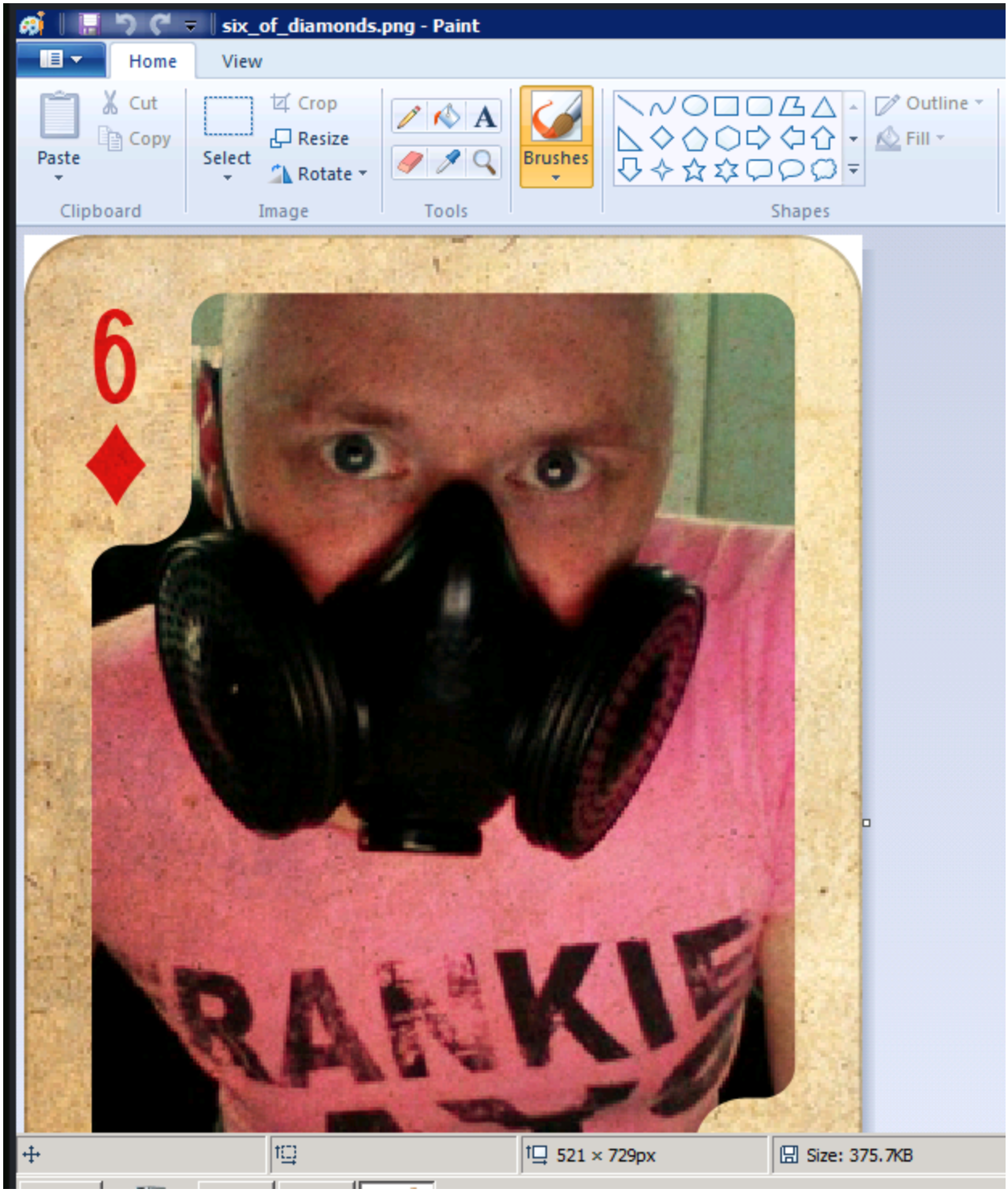
ftp -took hahaha.jpg

- 

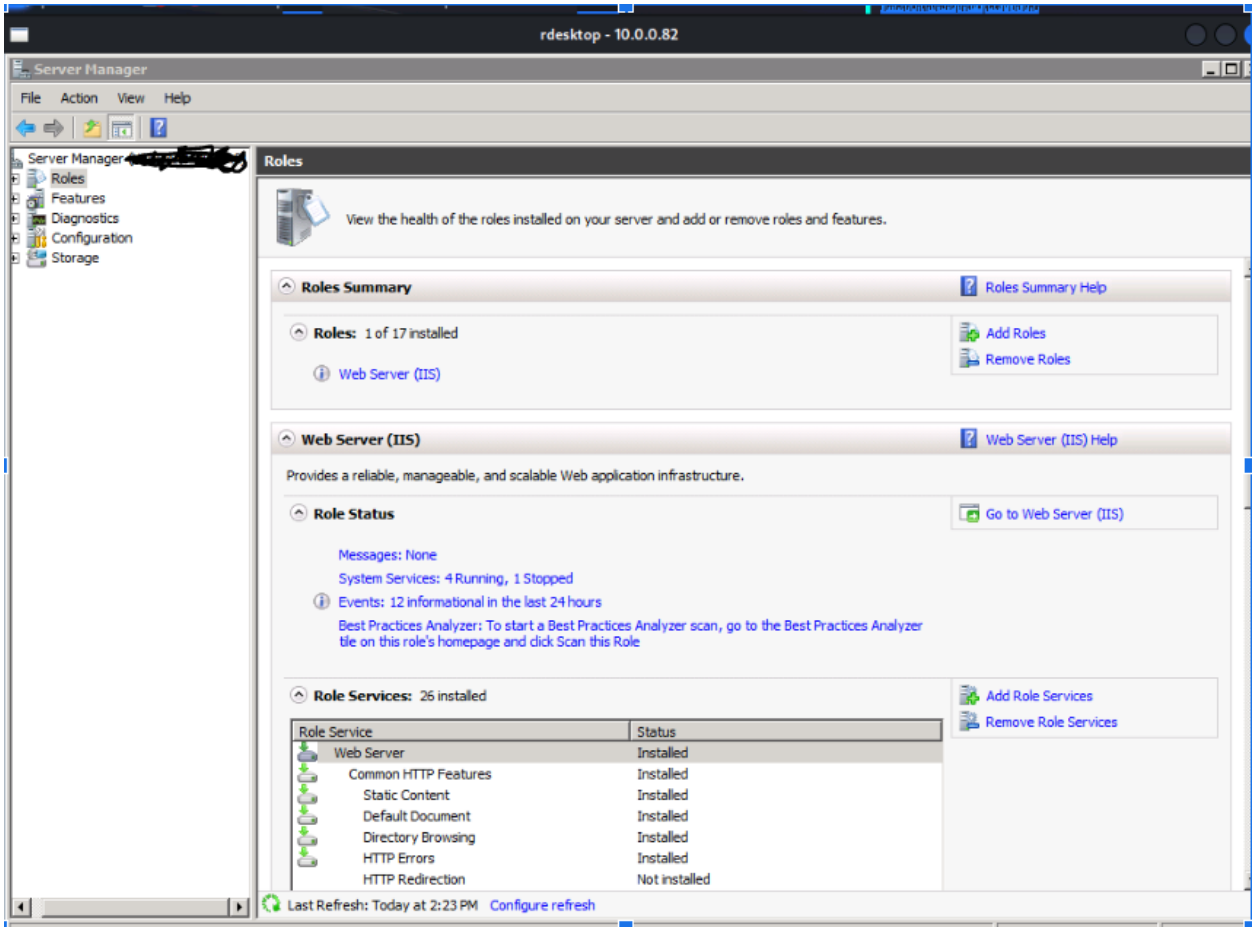
classified jack_of_hearts.docx



-
    - explioted password protected file six_of_diamonds.png inside six_of_diamonds.zip, pwd:vagrant

- 
six_of_diamonds.png - Paint
Home
View
Cut
Copy
Paste
Clipboard
Select
Crop
Resize
Rotate
Image
Tools
Brushes
Outline
Fill
Shapes
6
521 × 729px
Size: 375.7KB

Accessed Server Manager

- Attained all user names
- Able to check group membership
- Privilege escalation performed
- 

4.0 Maintaining Access

As Binary Bandits 01, preserving access to the compromised system at IP address 10.0.0.82 is a crucial aspect of our penetration test. It is imperative that we maintain the ability to re-enter this specific system even after it has been successfully exploited. This phase of the penetration test revolves around guaranteeing our continuous administrative control over the compromised system at IP address 10.0.0.82. Our goal is to establish persistent access methods that ensure our control remains intact, enabling us to conduct further assessments, gather valuable intelligence, and simulate real-world threat scenarios effectively.

5.0 House Cleaning

As Binary Bandits 01, our commitment to professionalism extends to the cleanup phase of our assessment, particularly on IP address 10.0.0.82. It is imperative that we leave no trace of our penetration test behind on this specific system, ensuring the utmost discretion and security for our clients.

During this phase, our primary goal is to meticulously remove any remnants of our presence from IP address 10.0.0.82. This includes eliminating any artifacts, tools, or user accounts that were created or manipulated during the penetration test. We understand that leaving behind fragments of our activities on an organization's computer can potentially lead to security issues in the future.

Upon successfully collecting trophies and achieving our assessment objectives on IP address 10.0.0.82, our team diligently removes all traces of our presence. It is our commitment that Offensive Security, our client, should not need to undertake any additional cleanup efforts as a result of our engagement on this specific system.

By conducting thorough house cleaning, we demonstrate our professionalism, respect for client environments, and commitment to ensuring that our penetration test activities have no adverse impact on the security and integrity of the systems we assess, including IP address 10.0.0.82.

6.0 Conclusion

Binary Bandits 01, on behalf of Simcorp, executed a comprehensive internal penetration test focusing on IP address 10.0.0.82. The team consisted of Natasha Siramarco, David Prutch, Raheem Reed, and Dustin Haggett. Our objective was to assess security and provide insights specific to this system.

Key Findings:

- Identified vulnerabilities on IP address 10.0.0.82.
- Strongly recommend addressing these promptly for improved security.

Assessment Highlights:

- In-depth examination of open ports, services, and potential vulnerabilities on IP address 10.0.0.82.
- Meticulous approach to uncover system details on IP address 10.0.0.82.

In summary, Binary Bandits 01 is dedicated to delivering professional penetration tests. We prioritize security and provide actionable insights. We stand ready to assist Simcorp in enhancing its cybersecurity posture, with specific attention to IP address 10.0.0.82.