Windows Server 2008 Report

REPORT BY – CHANDRA KANT BAURI

Target IP- 192.168.43.177

CRITICAL	HIGH	MEDIUM
3	1	1

Host Information:

NetBIOS Name: WIN-KAVQ59H6PK1

IP: 192.168.43.177

MAC Address: [redacted]

OS: Microsoft Windows Server 2008 Enterprise Service Pack 1

Nmap Scan:

```
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows Server (R) 2008 Enterprise 6001 Service
Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:0C:29:C8:AC:4B (VMware)
Service Info: Host: WIN-KAVQ59H6PK1; OS: Windows; CPE: cpe:/o:microsoft:wind
ows, cpe:/o:microsoft:windows_server_2008:r2

Host script results:
|_clock-skew: mean: -1h49m59s, deviation: 3h10m30s, median: 0s
| smb2-security-mode:
|   2.0.2:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-03-25T13:00:24
|_  start_date: 2022-03-25T12:27:23
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: WIN-KAVQ59H6PK1, NetBIOS user: <unknown>, NetBIOS MA
C: 00:0c:29:c8:ac:4b (VMware)
| Names:
|   WIN-KAVQ59H6PK1<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WIN-KAVQ59H6PK1<20>  Flags: <unique><active>
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Enterprise 6001 Service Pack 1 (Windows Serv
er (R) 2008 Enterprise 6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: WIN-KAVQ59H6PK1
|   NetBIOS computer name: WIN-KAVQ59H6PK1\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-03-25T18:30:24+05:30
```

Vulnerabilities :

No.	Severity	Vulnerability	Count
1.	Critical	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (EDUCATEDSCHOLAR) (uncredentialed check)	1
2.	Critical	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	1
3.	Critical	Unsupported Windows OS (remote)	1
4.	High	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	1
5.	Medium	SMB Signing not required	1

1. 40887 - MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (EDUCATEDSCHOLAR) (uncredentialed check)

Description:

The remote host is running a version of Microsoft Windows Vista or Windows Server 2008 that contains a vulnerability in its SMBv2 implementation. An attacker can exploit this flaw to disable the remote host or to execute arbitrary code on it.

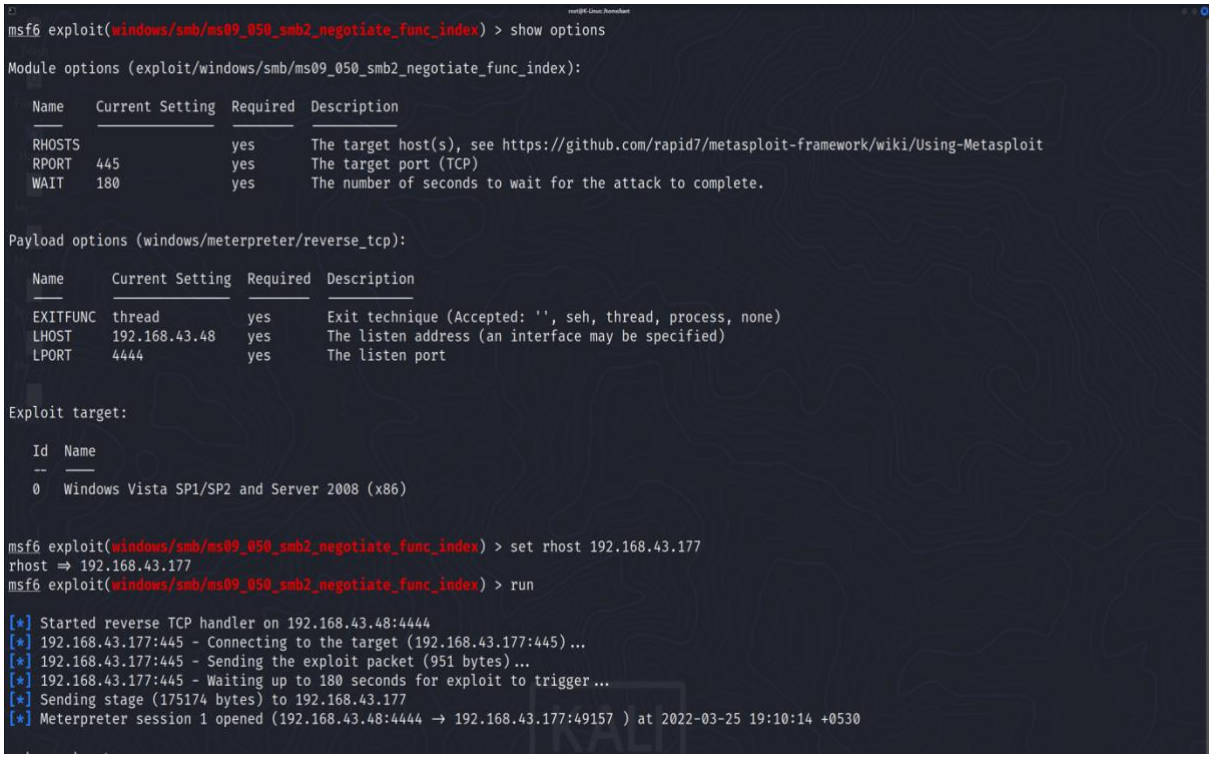
EDUCATEDSCHOLAR is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

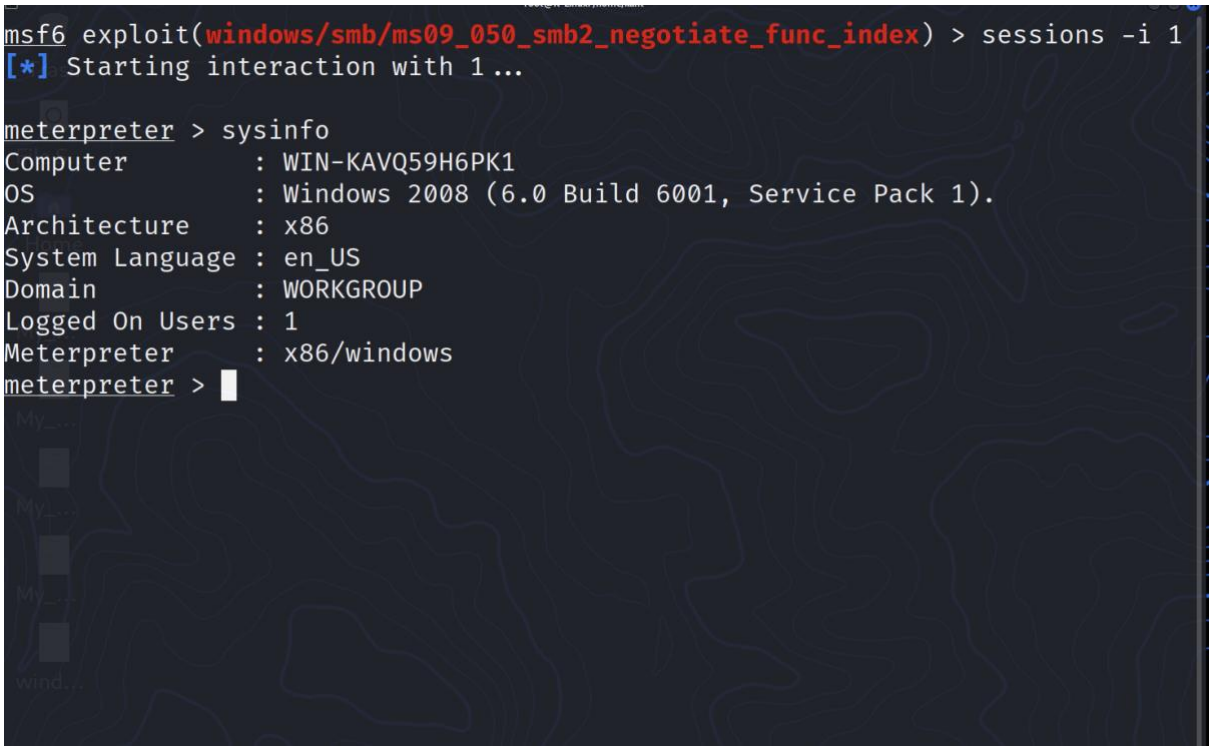
Exploitable With

Metasploit (MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference)

Port: 445/tcp

POC:





Note - After 180 second it will trigger the exploit and you will get a shell connection from windows server of the root user(System32).

CVSS v3.0 Base Score

Solution:

Microsoft has released a patch for Windows Vista and Windows Server 2008.

---

2. MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Description:

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the Network Service account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

Exploitable With

Metasploit (Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS)

Core Impact

CVSS v2.0 Base Score

Port: 5355 / udp / llmnr

Solution:

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.**)**

---

3. Unsupported Windows OS (remote)

Description:

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

CVSS v3.0 Base Score

Solution:

Upgrade to a supported service pack or operating system.

---

4. MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Description:

The remote Windows host is affected by the following vulnerabilities :
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

CVSS v3.0 Base Score

Port: 445 / tcp

Solution:

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

---

5. SMB Signing not required

Description:

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution:

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.