

RED / BLUE Team Exercise & Report  


## 

## 

## 

## 

**Contents**

[Exercise Agenda 3](#_Toc139936009)

[Reason for the exercise 3](#_Toc139936010)

[Scope 3](#_Toc139936011)

[Target Network 3](#_Toc139936012)

[Aim 4](#_Toc139936013)

[Objectives 4](#_Toc139936014)

[Team Member Names 4](#_Toc139936015)

[Exercise Methodology 4](#_Toc139936016)

[Denial of Service Attack 4](#_Toc139936017)

[Brute force Attack (Via SSH) 4](#_Toc139936018)

[Phishing Virus / Malware attack 5](#_Toc139936019)

[Supporting documentation 5](#_Toc139936020)

[Logistics 5](#_Toc139936021)

[Scenario 5](#_Toc139936022)

[Organizational Management Parties Involved 5](#_Toc139936023)

[Team Objectives 5](#_Toc139936024)

[Red Team 5](#_Toc139936025)

[Blue Team 5](#_Toc139936026)

[Master Scenario Events List 6](#_Toc139936027)

[Denial of Service Attack 6](#_Toc139936028)

[Brute Force Attack (SSH) 6](#_Toc139936029)

[Virus / Malware Attack 6](#_Toc139936030)

[Functional Exercise Injects 7](#_Toc139936031)

[Inject # 1 – Distributed Denial of Service (DDoS) Attack 7](#_Toc139936032)

[Inject # 2 – Brute Force Attack (SSH) 7](#_Toc139936033)

[Inject # 3 – Virus / Malware Attack 7](#_Toc139936034)

[Functional Exercise Inject Tracking Form 9](#_Toc139936035)

[Appendix A - Pre-exercise training strategy 11](#_Toc139936036)

[Distributed Denial of Service (DDoS) Attack 11](#_Toc139936037)

[SSH Brute-Force Attack 12](#_Toc139936038)

[Virus / Malware Attack 14](#_Toc139936039)

[Appendix B – Exercise evaluation 15](#_Toc139936040)

[Red Team 17](#_Toc139936041)

[Blue Team 18](#_Toc139936042)

[Conclusion 19](#_Toc139936043)

[Summary of Findings 21](#_Toc139936044)

[Attack Success Rate 21](#_Toc139936045)

[Defensive Measures Effectiveness 21](#_Toc139936046)

[Risk Assessment 22](#_Toc139936047)

[Recommendations 22](#_Toc139936048)

[Lessons Learnt 22](#_Toc139936049)

[Executive Summary 23](#_Toc139936050)

|  |
| --- |
| Exercise Agenda |

## 

|  |
| --- |
| Reason for the exercise |

This exercise will evaluate the readiness and response of the Incident Response Team against three incident types. The purpose of these exercises is to support the training of OzCasual staff in the operation of the new infrastructure. The outcomes of these exercises will help evaluate the performance of the security measures that have been implemented by SecureNET.

## 

|  |
| --- |
| Scope |

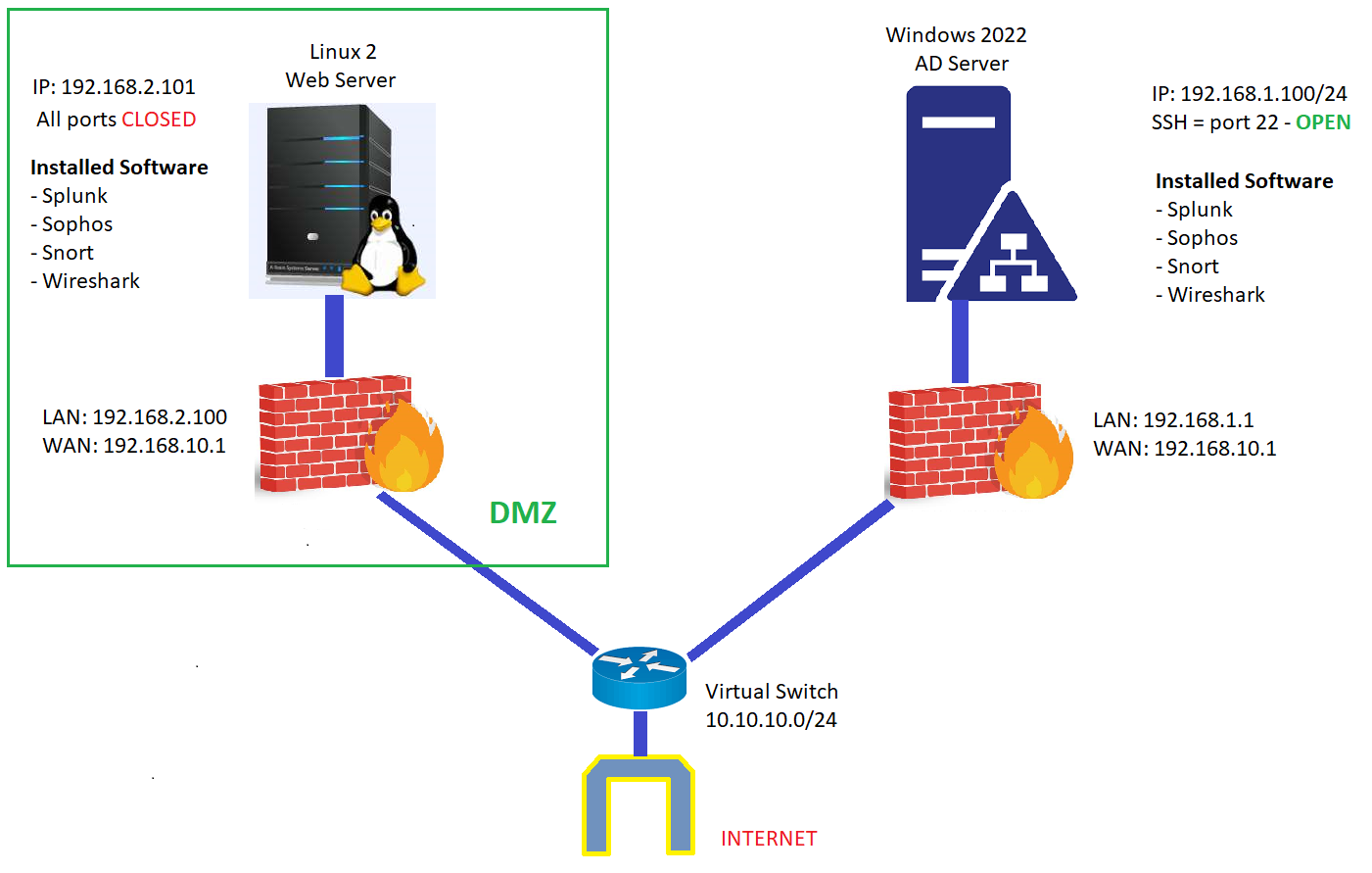
For the purposes of this exercise, the simulation will be conducted in a virtual environment using VM Box virtual environment, containing:

* Windows AD - Server
* Linux Web – Server
* PFSense Firewall

## 

|  |
| --- |
| Target Network |

## 



A Kali Linux instance will be used to perform scans and attacks on the target network and test responses to the following three cybersecurity incidents:

1. A Denial of Service Attack on the Windows AD server
2. A Brute force Attack (Via SSH) on the Linux Web Server
3. A Phishing Virus / Malware attack on the Windows AD server

## 

|  |
| --- |
| Aim |

The aim of this exercise is to train the OzCasual staff in the new infrastructure implemented to protect the new architecture. This will also reveal the repercussions of a successful breach, and the damage it can do company wide.

The simulation will allow the ICT staff at OzCazual to experience and condition themselves to an attack, so if the company was to come under a real world attack, they would have experience in understanding their roles and improving their response. The hope is, after the exercises have been successfully tested on the OzCazual staff, it can allow them to make the necessary changes to their knowledge of cyber response and hygiene, and prevent the company falling victim to an attacker.

## 

|  |
| --- |
| Objectives |

## 

1. Utilize the the Incident Management Plan created and assess the effectiveness and response of the ICT
2. Assess the effectiveness of the updated procedures in the runbooks
3. Document and review incident responses and make revisions where necessary, to improve the response and effectiveness of the IRT
4. Identify areas requiring further training, not just for the IRT, but for all staff and management
5. Collaborate post-simulation, to assess areas the IRT can improve and further training

|  |  |
| --- | --- |
| Team Member Names | |
| Giuseppe Raciti | Project Manager / Team Lead |
| Mauricio G. Guerra | Server Administrator |
| Shaun Heywood | Cyber Security Specialist |
| Mark Byrne | Cloud Architect / Engineer |

## 

|  |
| --- |
| Exercise Methodology |

### Denial of Service Attack

Using the Kali Linux VM:

* A nmap scan will be conducted by the Read Team to the targeted Linux Web Server.
* The nmap scan will reveal the opened ports that the Read Team will use to perform a DOS attack.
* The Read Team will perform the attack from Kali to the targeted Linux Web Server.

### Brute force Attack (Via SSH)

Using the Kali Linux VM:

* A scan will be conducted on the target system to identify any open ssh ports
* Once on open port is identified, a brute force attack will performed using Metasploit
* Metasploit will use existing or well known username and password files to find a match and gain root access.

### Phishing Virus / Malware attack

Using the Kali Linux VM:

* A Phishing email will be created using the Social Engineering Toolkit (SET) that will contain a virus / malware payload
* The phishing email will be sent to the target [cyberclass2023@outlook.com](mailto:cyberclass2023@outlook.com), which will be located on the Windows Server
* The payload will be run by the email user, infecting the Windows Server with a virus

|  |
| --- |
| Supporting documentation |

* Denial of Service Response Runbook
* Phishing Incident Response Runbook
* Ransomware Incident Response Runbook

## 

|  |
| --- |
| Logistics |

The exercise will require the use of the VM Box cloud-based hosting service of VM’s, which during the exercise will be accessed one at a time by each member of the red and blue teams. One person will host the VM, and provide the rest of the members with a link that will give them access to the remote desktop into the environment..

The red team will begin by initiating their attack. After the red team has performed a critical action in the exercise, the red team will log off, allowing the blue team to connect and perform their defensive measures.

## 

|  |
| --- |
| Scenario |

In a simulated cyber-attack, the OzCasual IRT red team of skilled hackers, will scan the network looking for vulnerabilities, before initiating a number of attacks against the target organization's environment. The red team will attempt to interrupt or access both the Linux Web Server and Windows AD server.

## 

|  |
| --- |
| Organizational Management Parties Involved |

## 

* **Red Team**

The red team has been allocated a Kali Linux ‘attacker’ machine

* **Blue Team**

The blue team will be responsible for the OzCasual secure environment which is the ‘target’ environment.

## 

|  |
| --- |
| Team Objectives |

### Red Team

* **Deny Access:** Prevent users from accessing the environment via a DoS attack
* **Gaining unauthorized access:** Gain access to the target organization's network or systems, evading security measures, and obtaining access privileges.
* **Maintain persistence:** Once inside the target network is to establish persistence by keeping access and avoiding detection.
* **Infect and Execute:** The red team will install and execute the malware

### Blue Team

* **Detect and Prevent:** The blue team's main goal is to detect and prevent any cyber attacks on the OzCasual network
* **Respond:** React quickly and in the case of a successful cyberattack, contain the damage, isolate the afflicted systems, and stop malware from spreading
* **Remove and Disable:** The blue team will need to remove the infected files from the compromised system, and disable the attack vector.
* **Investigate:** To fully understand the attack paths, the level of compromise, and any potential vulnerabilities, the blue team will conduct an in-depth investigation into any cyber inciden

|  |
| --- |
| Master Scenario Events List |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Event #** | **Team** | **MSEL Key Event Description** | **Injects and  Expected Actions** | **Objectives** |
| Denial of Service Attack | | | | |
| ***1*** | Red | Perform nmap on the target server 124.187.235.214 |  | Identify open ports that could be used for an attack |
| ***2*** | Blue | Monitor if Snort (IDS/IPS) detect any incoming data from the nmap scan |  | Establish a baseline of traffic before the attack |
| ***3*** | Red | With the information from the nmap scan select a port to perform the DOS attack. |  | Exploit the identified point of attack |
| ***4*** | Red | Carry out a DOS attack from Kali | **INJECT #1** | Attempt to disrupt or crash the server |
| ***5*** | Blue | Monitor how Sophos XG Firewall block the incoming pings using Splunk Software | **BLOCK PINGS** | Verify the security measures are preventing the attack |
| ***6*** | Blue | Monitor how Snort (IDS/IPS) performs with the incoming pings |  | Verify logs that the firewall prevented further entry |
| Brute Force Attack (SSH) | | | | |
| ***1*** | Red | Perform nMap scan on the target server 192.168.2.101 |  | Identify open ports that could be used for a brute force attack |
| ***2*** | Blue | Monitors for scans via Snort and provides alert |  | Collects evidence of scans |
| ***3*** | Red | Identify if any open ssh ports |  | Identify vulnerability |
| ***4*** | Red | Run Brute Force attack on open port using sample username and password list files | **INJECT #2** | Gain root access to Linux Web server |
| ***5*** | Blue | Monitor for multiple login attempts in Splunk |  | Identify attack and collect evidence |
| ***6*** | Blue | Block malicious connections and record connection details | **BLOCK CONNECTION** | Block active connection, noting details of IP address, domain |
| Virus / Malware Attack | | | | |
| ***1*** | Red | Create virus / malware payload using Social Engineering Toolkit (SET) |  | create a virus |
| ***2*** | Red | Create phishing email using Social Engineering Toolkit (SET) |  | create an email to send to the target |
| ***3*** | Red | Attach payload to phishing email using Social Engineering Toolkit (SET) |  | attach virus to email |
| ***4*** | Red | Deploy phishing email to target using Social Engineering Toolkit (SET) | **INJECT #3** | send the phishing email to the target |
| ***5*** | Blue | Monitor for phishing emails, and / or virus and malware in Sophos |  | keep a lookout for suspicious activity |
| ***6*** | Blue | Phishing email detected and cleaned with Sophos, logged with Splunk | **Detect and Clean** | detect and clean the threat, check it is logged in Splunk |

*The MSEL lists key scenario events, expected Injects that will build on the key events, and the objectives of each MSEL item.*

*Controllers, simulators, and data collectors will refer to the MSEL throughout the exercise to ensure the exercise remains on tr*

|  |
| --- |
| Functional Exercise Injects |

|  |  |  |  |
| --- | --- | --- | --- |
| Inject # 1 – Distributed Denial of Service (DDoS) Attack | | | |
| **Date/Time of inject:** | Sunday, 9th July 2023 14.00 Hrs | |  |
| **From:** | Kali Linux (Attacking Machine) | |  |
| **To:** | Linux Web Server | |  |
| Organization management correspondence: | | OzCazual Project Owner | |
| Method of injection: DOS Attack | | | |
| * Red team will scan the Linux Web Server for open ports * After an open port has been detected, Red Team will perform the attack * Using Kali Linux the DOS attack will be performed using command lines previously tested * The attack will be on track if the Linux Web Server stop working | | | |

## 

## 

|  |  |  |  |
| --- | --- | --- | --- |
| Inject # 2 – Brute Force Attack (SSH) | | | |
| **Date/Time of inject:** | Sunday, 9th July 2023 14.00 Hrs | |  |
| **From:** | Kali Linux (Attacking Machine) | |  |
| **To:** | Linux Web Server | |  |
| Organization management correspondence: | | OzCazual Project Owner | |
| Method of injection: Brute Force SSH | | | |
| * The attacker will scan for open SSH ports * If an open ssh port is identified, the attacker will use Kali brute force attack tools * The Brute force tools will use a list of common usernames and passwords to repeatedly try and gain access to the target machine. * If successful the attacker will aim to bring down the Web Server | | | |

## 

## 

|  |  |  |  |
| --- | --- | --- | --- |
| Inject # 3 – Virus / Malware Attack | | | |
| **Date/Time of inject:** | Sunday, 9th July 2023 14.00 Hrs | |  |
| **From:** | Kali Linux (Attacking Machine) | |  |
| **To:** | Windows Server | |  |
| Organization management correspondence: | | OzCazual Project Owner | |
| Method of injection: Phishing virus / malware file | | | |
| * Social Engineering Toolkit used on the Kali attacker to create a payload * Social Engineering Toolkit used on the Kali attacker to create a phishing email * Phishing email sent to the target, [cyberclass2023@outlook.com](mailto:cyberclass2023@outlook.com) * Target did not receive the email as it was blocked by Sophos | | | |

|  |
| --- |
| Functional Exercise Inject Tracking Form |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | **Inject Tracking Form** |  |
| **Inject #** | **Scheduled Inject Time** | **Actual Inject Time** | **Inject Summary** | **Comments** |
| **1** | 9th July 2023  15.00 Hrs | 9th July 2023  12:30 Hrs | The nmap scan was performed to the target: 124.187.235.214. We found the following ports open: 67, 68, 80, 1900, 3389, all of them UDP.    The DOS attack was performed | The DOS attack was blocked by Sophos XG Firewall. The DOS attack was unsuccessful. |
| ***2*** | 9th July 2023  14.00 Hrs | 9th July 2023 13.35 Hrs | nMap was performed on the target network 124.187.235.214 and no SSH ports were found to be open. Unable to perform a Brute Force SSH attack | To confirm this was blocked the Brute Force attack was carried out regardless and failed: |
| ***3*** | 9th July 2023  16.00 Hrs |  |  | The phishing attack with the virus / malware payload was successfully detected and removed |

|  |
| --- |
| Appendix A - Pre-exercise training strategy |

## 

|  |
| --- |
| Distributed Denial of Service (DDoS) Attack |

|  |
| --- |
| **Red Team** |
| **Background:**  A DOS (Denial of Service) attack is a malicious act that aims to disrupt the availability of a computer system or network by overwhelming it with a flood of illegitimate requests or traffic. By consuming the target's resources to the point of exhaustion.  To attack the vulnerable machine you need the IP address of the target and flood it with pings using Kali Linux.  **Tools and Techniques:**  To perform the DOS attack you have to use the following tools:   * nmap * hping3   Steps to perform the DOS attack using Kali Linux:  **Step One**: Perform an NMAP scan to get the list of open ports on the target machine  $ nmap -sS -sV 124.187.235.214  This will provide the list of all the open ports and services running on them.  **Step Two**: After the NMAP has been performed, test each of the open ports. Example:  67/udp open  68/udp open  80/udp open  **Step Three**: Use the following command to perform the DOS attack:  sudo hping3 -S -p 80 -c 50 124.187.235.214 –rand-source |
| **Blue Team** |
| The implemented security measures were effective in mitigating the attack, preventing any significant disruption to the availability of the targeted server. The logs in Splunk clearly indicate the increased traffic caused by the attack, allowing the Blue Team to identify and respond to the incident promptly    Despite the unsuccessful DoS attack, by diligently investigating the incident and implementing appropriate enhancements, the Blue Team can strengthen the server's defenses and better protect against future attacks. |

|  |
| --- |
| SSH Brute-Force Attack |

|  |
| --- |
| **Red Team** |
| **Background:**  The Secure Shell Protocol (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Its applications are remote login and command-line execution. SSH protocols are based on the client-server architecture, i.e the SSH client and the SSH server.  To gain access to the vulnerable machine you need the address of the machine or the name of the machine. To gain access to the machine you need the correct combination of username and password. You will need to make or use two different text files one for possible usernames and one for the possible passwords.  **Tools and Techniques:**  Once you have these three elements Kalil Linux has a number of tools to perform the Brute Force Attack, including:   * sudo * Hydra, * Medusa * Ncrack   Steps to perform the SSH Bruteforce Attack using Metasploit:  **Step One**: Please check the Metasploit is properly installed and update if required through the below command  apt-get update && apt-get upgrade  **Step two**: Perform an NMAP scan to get the list of open ports on the target machine  $ nmap -sS -sV 192.168.2.101 (The target machine address)  This will provide the list of all the open ports and services running on them.  **Identify any open ports that are running an SSH service**  **Step three**: Launch Metasploit through the following command  sudo msfconsole  **Step four**: Search for ssh\_login Auxiliaries by using the Search command in msfconsole  search ssh  **Step five**: use the auxiliary/scanner/ssh/ssh\_login from the results, through the following command  msf6 > use auxiliary/scanner/ssh/ssh\_login  **Step six**: Use the options available to set our target, to see the options use the command Show options  msf6 > (auxiliary/scanner/ssh/ssh\_login) > show options  **Step seven**: Use the below commands to set any desired options  msf6 > (auxiliary/scanner/ssh/ssh\_login) > set RHOST 192.168.10.3  msf6 > (auxiliary/scanner/ssh/ssh\_login) > set THREADS 3  msf6 > (auxiliary/scanner/ssh/ssh\_login) > set STOP\_ON\_SUCCESS true  msf6 > (auxiliary/scanner/ssh/ssh\_login) > set VERBOSE true  **Step eight**: Set the path for the usernames and password lists based on the location of these files)  msf6 > (auxiliary/scanner/ssh/ssh\_login) > set PASS\_FILE /root/Desktop/passwords.txt  msf6 > (auxiliary/scanner/ssh/ssh\_login) > set USER\_FILE /root/Desktop/usernames.txt    **Step nine**: run the brute force attack  msf6 > (auxiliary/scanner/ssh/ssh\_login) > run |

### 

|  |
| --- |
| **Blue Team** |
| The blue team demonstrated a strong defense against the SSH Brute Force Attack performed by the red team during the pen test simulation. The Linux webserver was equipped with several security measures, including a Sophos Firewall, Sophos Intercept X, Snort, and Splunk, which played crucial roles in thwarting the attack  Despite the red team utilizing tools like Hydra, Medusa, and Ncrack to perform the Brute Force Attack, the blue team's security measures and configuration prevented the unauthorized access to the vulnerable machine. The attack was unable to find the correct combination of usernames and passwords to gain access, as the blue team had implemented strong security practices.    The blue team's security infrastructure effectively logged and monitored the network traffic, as evidenced by the Splunk logs showing a spike in activity during the time of the attack. The Sophos Firewall provided an additional layer of protection, successfully blocking the malicious SSH login attempts  The blue team's ability to detect and log the attack within Splunk showcases their proactive monitoring and incident response capabilities. The successful defense against the SSH Brute Force Attack highlights the effectiveness of the security measures in place, including the Sophos Firewall and Snort, which detected and mitigated the threat. |

## 

|  |
| --- |
| Virus / Malware Attack |

|  |
| --- |
| **Red Team** |
| During the pen test simulation, the red team employed a Kali Linux system to create and distribute a phishing email containing malicious software. The target of the attack was a Windows 2022 Active Directory (AD) server, shielded by a pfSense firewall and fortified with security software, including Sophos antivirus, Snort, Splunk, and Windows Defender.  The phishing email was sent to the email address cyberclass2023@outlook.com. Unfortunately, the recipient fell victim to the deception and opened the email attachment. However, the blue team, responsible for defending the system, promptly detected and removed the malicious content, successfully mitigating the potential risk.  The installed Sophos antivirus software proved to be a crucial defense mechanism, as it swiftly identified the threat upon the email's opening and promptly took action to neutralize it. The blue team effectively leveraged their security infrastructure, including Sophos, to prevent any further compromise of the Windows 2022 AD server |
|  |
| **Blue Team** |
| The phishing email was sent to the email address cyberclass2023@outlook.com, and the targeted user fell for the deception and opened the attachment. However, the blue team, responsible for defending the system, quickly responded to the threat. Sophos, the installed antivirus software, promptly detected the presence of the virus and prevented the download from completing. It then took further action by quarantining and ultimately deleting the malicious file.  The blue team effectively leveraged Sophos Central, a centralized management console, to monitor and review the security event. By analyzing the Sophos firewall log, they were able to identify the detected virus and document the appropriate actions taken to mitigate the threat.    Overall, the blue team demonstrated a high level of competence in incident response and defense mechanisms. Their proactive monitoring and swift action in halting the attack, combined with their effective utilization of security tools, contributed to the successful prevention of a potentially harmful intrusion.  In a real-world scenario however, it would be ideal that the person who open the malicious email would require training on good practices for Cyber Hygiene, and educate them on awareness of phishing emails. |

|  |
| --- |
| Appendix B – Exercise evaluation |
| Red Team |
| **Activity name:** Functional Exercise for DDoS attack, Brute Force SSH attack, and Phishing and Virus attack |
| **Did you have available to you all of the information and resources needed to fulfill your responsibilities?  If so, comment on its suitability. If not, provide details of what was missing.** |
| In terms of information and resources, we had access to all necessary tools and details to fulfill our responsibilities as a penetration tester. The presence of the Sophos Firewall successfully blocking the DoS attack and the Brute Force SSH attack indicated that the system was equipped with robust protection measures. This suggests that the information and resources provided were suitable for evaluating the effectiveness of the system's defenses against such attacks. |
| **Did you feel that there was an adequate level of training to support the attack? If, not provide details** |
| The level of training provided for the attack was adequate, as demonstrated by the firewall's ability to stop the DoS and Brute Force SSH attacks. It indicates that the personnel responsible for system security had received sufficient training to configure and maintain the firewall effectively. The fact that the attacks were blocked highlights the effectiveness of the training in preparing the team to detect and mitigate potential threats. |
| **Was the structure of the exercise realistic? If not, provide details** |
| The structure of the exercise was realistic, given the results. The presence of a Sophos Antivirus system that detected and removed the phishing attack's malware payload reflects a well-designed exercise that mirrors real-world scenarios. The exercise effectively tested the system's ability to identify and respond to phishing attempts, providing valuable insights into the organization's security posture and the effectiveness of its defense mechanisms. |
| **How can the red team’s actions be improved?** |
| There are various approaches to improve the red team's actions in a red team / blue team penetration test. They could improve their reconnaissance efforts by completing thorough research about the target organization's infrastructure, staff, and technologies.  Next, the red team should aim to simulate genuine attack scenarios by replicating the techniques used by actual threat actors. This involves coordinating their actions, testing all layers of security controls, collaborating with the blue team, and providing detailed reports with actionable recommendations.  Finally, continual learning and adaptation are required for the red team to stay current on the latest attack methodologies and defensive strategies, ensuring that the pen test stays effective in analyzing the organization's security posture |
| **How can the red team’s training be improved?** |
| To improve the red team’s training, key measures to undertake could include developing diverse skills, conducting realistic scenario simulations, encouraging collaboration and feedback between team members, continuous professional development, and promoting ethical conduct. These improvements can help create skilled and adaptable red teams that can effectively simulate real-world threats and enhance the overall security posture of the organization.. |
| **How appropriate was the pre-training to the exercise?** |
| The red team's pre- training was considered highly appropriate for the exercise, as the team conducted in depth tests of both applications and exploits, which contributed to such a successful exercise for the organization. |
| **How could the pre-training be improved?** |
| To improve pre-training for red teams, the focus could be placed on;   * · identifying training gaps by conducting a needs assessment * · developing a customised learning program covering technical and non-technical topics * · incorporating practical hands-on exercises * · providing access to training tools and resources * · promoting mentorship and collaboration within the team * · implementing continuous evaluation and feedback   These improvements can help ensure red team members receive targeted and relevant training, equipping them with the knowledge and skills needed for effective engagement in security assessments. |

|  |
| --- |
| Blue Team |
| **Activity name:** Functional Exercise for DDoS attack, Brute Force SSH attack, and Phishing and Virus attack |
| **Did you have available to you all of the information and resources needed to fulfill your responsibilities? If so, what information and resources were used? If not, provide details of what was included and what should have been included** |
| Yes. With all the security software installed, such as Splunk, Snort, Sophos (firewall and antivirus) and Wireshark, all three attacks were unsuccessful in their attempts. |
| **Did you feel that there was an adequate level of training to support the response effort? If, not provide details** |
| As with any software, an intimate knowledge of its workings and functionality, would allow better understanding of the logs and alerts that any of the security software raised an alert for |
| **Was the structure of the exercise realistic? If not, provide details** |
| Yes. With the set up being as close to realistic as possible |
| **Please provide comments regarding what you believe worked and did not work during the exercise?** |
| Snort was one of the programs that requires extreme fine tuning, therefore a better knowledge of the software could help make alerts easier and more concise to read. The alternative is a different software performing the same function |
| **How can the blue team’s response be improved?** |
| Sine both systems were being monitored in real-time, setting up all the software to raise alerts for potentially malicious activity, would be more ideal, rather than sit there knowing the attack was imminent |
| **How can the blue team’s training be improved?** |
| Education on the use of each security tool will allow for betting analysis of the information. |

|  |
| --- |
| Conclusion |
| Summary of Findings |
| During the functional exercise, our penetration testing team executed three distinct attacks to assess the security posture of the target systems. Firstly, the DoS attack aimed at a Linux Web Server was unsuccessful in its objective due to the robust defense mechanisms of the Sophos XG Firewall. The firewall effectively blocked the attack, showcasing its capability to withstand such malicious traffic.  Secondly, the Brute Force SSH attack, targeting the same Linux Web Server, was also thwarted by the Sophos XG Firewall. This outcome demonstrates the firewall's effectiveness in detecting and preventing unauthorized access attempts, safeguarding the server against brute force attacks.  Lastly, the phishing and virus attack directed at a Windows Server encountered resistance from the Sophos Antivirus system. The phishing attempt was detected, and the associated malware payload was promptly identified and removed. This highlights the efficacy of the antivirus solution in recognizing and mitigating potential threats, enhancing the security posture of the Windows Server. |
| Attack Success Rate |
| The functional exercise conducted by our penetration testing team assessed the success rate of three distinct attacks targeting the designated systems. The DoS attack aimed at the Linux Web Server was rendered unsuccessful, as the Sophos XG Firewall effectively blocked the attack, preventing any disruption to the server's availability. Similarly, the Brute Force SSH attack directed at the same Linux Web Server was efficiently thwarted by the firewall, effectively protecting the server from unauthorized access attempts.  In the case of the phishing and virus attack, which targeted the Windows Server, the Sophos Antivirus system successfully detected the phishing attempt and promptly identified and removed the associated malware payload. This highlights the strong detection capabilities of the antivirus solution, ensuring the protection of the Windows Server against potential compromise.  The attack success rate for the functional exercise was notably low, with the security measures in place effectively mitigating the risks posed by the simulated attacks. The Sophos XG Firewall and Sophos Antivirus demonstrated their effectiveness in safeguarding the targeted systems, emphasizing the importance of robust security solutions in defending against DoS attacks, Brute Force SSH attacks, and phishing attempts. |
| Defensive Measures Effectiveness |
| The functional exercise conducted at OzCasual assessed the effectiveness of defensive measures implemented to protect the organization's infrastructure against cybersecurity incidents. The exercise focused on evaluating the response to a Denial of Service (DoS) attack, Brute Force SSH attack, and Phishing Virus/Malware attack.  The defensive measures implemented, including the Sophos XG Firewall, Snort (IDS/IPS), Splunk enterprise, Sophos Antivirus, and other security tools, demonstrated their effectiveness in detecting, blocking, and responding to the simulated attacks.  The Sophos XG Firewall successfully blocked the DoS attack, preventing any disruption to the availability of the targeted server. It demonstrated its capability to withstand a flood of illegitimate requests and effectively protected the infrastructure.  Similarly, the Sophos XG Firewall and Snort (IDS/IPS) successfully detected and prevented the Brute Force SSH attack. The intrusion detection and prevention systems promptly identified the unauthorized access attempts and took appropriate actions to prevent compromise.  The Sophos Antivirus system proved to be a robust defense mechanism against the Phishing Virus/Malware attack. It detected the phishing attempt and promptly removed the associated malware payload, ensuring the security of the targeted system.  The integration of Splunk enterprise as a centralized logging and monitoring tool provided valuable insights into potential security incidents. It enabled the blue team to proactively monitor the network, detect suspicious activities, and respond promptly to mitigate threats.  Overall, the defensive measures demonstrated their effectiveness in protecting the organization's infrastructure during the exercise. However, recommendations for improvement include enhancing firewall configurations, fine-tuning Snort (IDS/IPS) alerts, improving logging and monitoring capabilities, and conducting regular training and awareness programs to ensure optimal utilization of the security tools |
| Risk Assessment |
| The risk assessment conducted during the functional exercise identified potential risks and vulnerabilities within the OzCasual infrastructure. The assessment focused on the three simulated cybersecurity incidents: a Denial of Service (DoS) attack, a Brute Force SSH attack, and a Phishing Virus/Malware attack.  Based on the exercise, the following risk areas were identified:  **DoS Attack**: The risk of a successful DoS attack was mitigated by the effectiveness of the Sophos XG Firewall in blocking the attack and maintaining the availability of the targeted server. However, continuous monitoring and fine-tuning of firewall configurations are recommended to ensure optimal protection against future DoS attacks.  **Brute Force SSH Attack**: The risk of unauthorized access through a Brute Force SSH attack was successfully mitigated by the Sophos XG Firewall, which detected and prevented the attack. However, regular monitoring and updates to firewall rules, as well as implementing multi-factor authentication (MFA), are recommended to further enhance security and prevent potential unauthorized access.  **Phishing Virus/Malware Attack**: The risk of a successful phishing attack was effectively mitigated by the Sophos Antivirus system, which promptly detected and removed the malicious payload. However, ongoing training and awareness programs for employees to recognize and report phishing attempts are essential to minimize the risk of falling victim to such attacks. |
| Recommendations |
| 1. Conduct regular vulnerability assessments and penetration tests: Regular assessments and tests should be conducted to identify any weaknesses or vulnerabilities in the system. This will help in strengthening the security measures and ensuring that all potential attack vectors are addressed. 2. Enhance firewall configurations: Although the firewall was effective in blocking the attacks during the exercise, it is recommended to regularly review and update firewall configurations to ensure optimal protection. This includes monitoring and adjusting firewall rules, intrusion detection and prevention systems (IDS/IPS), and access control lists (ACLs) to match the evolving threat landscape. 3. Improve monitoring and logging capabilities: Enhance the monitoring and logging capabilities of security tools like Splunk to provide more detailed and actionable insights into potential security incidents. This will enable the blue team to detect and respond to threats more effectively. 4. Provide regular cybersecurity training and awareness programs: Educate all staff members, including IT and non-IT personnel, on cybersecurity best practices, such as recognizing and avoiding phishing emails, practicing good password hygiene, and reporting suspicious activities. Regular training programs will help create a culture of cybersecurity awareness within the organization. 5. Develop and test incident response plans: Continuously update and test incident response plans, including runbooks specific to different types of incidents. Regular exercises and simulations will help the incident response team improve their skills and coordination, ensuring a prompt and effective response in the event of a real cyber incident |
| Lessons Learnt |
| Robust security measures are crucial: The exercise demonstrated the importance of implementing and maintaining strong security measures, including firewalls, antivirus software, intrusion detection systems, and advanced threat detection solutions. These measures proved effective in detecting and mitigating the simulated attacks.  Proactive monitoring and incident response are essential: The blue team's ability to proactively monitor the network, detect potential threats, and respond promptly played a significant role in preventing successful attacks and minimizing the impact of the simulated incidents. Continual monitoring and real-time incident response are critical to maintaining a secure environment.  Regular training and awareness are key: The exercise highlighted the importance of ongoing training and awareness programs for all staff members. By educating employees about cybersecurity best practices and raising awareness about potential threats, organizations can significantly reduce the risk of successful attacks.  Continuous improvement is necessary: The exercise revealed areas for improvement in terms of fine-tuning security tools, enhancing logging and monitoring capabilities, and refining incident response processes. It is essential to regularly review and improve security measures to stay ahead of emerging threats and adapt to changing attack techniques |
| Executive Summary |
| The functional exercise successfully evaluated the readiness and response of the Incident Response Team (IRT) at OzCasual against three simulated cybersecurity incidents: a Denial of Service (DoS) attack, a Brute Force SSH attack, and a Phishing Virus/Malware attack. The exercise aimed to train the IRT and assess the effectiveness of the security measures implemented in the new infrastructure.  Overall, the exercise demonstrated the effectiveness of the security measures in place, as the red team's attacks were successfully mitigated by the blue team's defense mechanisms. The Sophos XG Firewall, Sophos Antivirus, Snort (IDS/IPS), and Splunk played crucial roles in detecting, blocking, and responding to the simulated attacks.  The exercise highlighted the importance of ongoing training, proactive monitoring, and continuous improvement in maintaining a strong security posture. It also identified areas for enhancement, such as firewall configurations, monitoring capabilities, and incident response processes.  By implementing the recommendations and lessons learned from the exercise, OzCasual can further strengthen their security measures, enhance incident response capabilities, and create a culture of cybersecurity awareness throughout the organization. These measures will help mitigate the risks posed by real-world cyber threats and ensure the protection of critical infrastructure and data |
|  |