Test Your Cyber Security Incident and Incident Response Skills! ANSWER KEY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Answer | Term |  | Letter | Description |
| J | Crisis Management |  | A | Procedure that treats the internal network as hostile, segmenting different organizational units or systems from each other. Often performed by host-based firewall, iptables, netsh advfirewall tools. |
| E | Isolation |  | B | Procedure to baseline a system and verify that is operating in a normal state. |
| O | User and Entity Behavior Analytics (UEBA) |  | C | Attack technique using the component of Microsoft **Windows** XP and later iterations of the operating systems, which facilitates asynchronous, prioritized, and throttled **transfer** of files between machines using idle network bandwidth. |
| A | Internal Segmentation |  | D | Attack technique that uses the Application Compatibility Toolkit to trick applications into not seeing the ports, directories, files, and services the attackers want to hide. |
| I | Real Intelligence Threat Analytics (RITA) Analysis |  | E | Procedure that uses various switch and router commands to quarantine infected system to prevent further harm. |
| M | Firewall Log Review |  | F | Brute force attack where the hacker tries to gain access to an organization’s systems by testing out a small number of commonly used passwords on many accounts, on the assumption that within a large group of people, there's likely to be at least one using a common password. |
| B | Server Analysis |  | G | Attackers create and load their malware using a service with SYSTEM privileges; or create a new service. |
| P | Domain Fronting |  | H | Attackers use a vulnerability in local software to gain administrative access. |
| C | Windows Background Intelligent Transfer Service (BITS) |  | I | Procedure that examines the network traffic, parsing and conduct a review.  |
| D | Application Shimming |  | J | Procedure by which an organization deals with a disruptive and unexpected event that threatens to harm the organization or its stakeholders. |
| L | Evil Firmware |  | K | Valid active directory credentials have been discovered on open shares and files within the environments that are used by attackers. |
| H | Local Privilege Escalation |  | L | Attackers update firmware of network cards, video cards, and BIOS or UEFL. |
| G | New Service Creation |  | M | Procedure that analyzes firewall logs. Regularly emulate attack scenarios to verify procedures. |
| K | Credential Stuffing |  | N | Attackers send a malicious email targeting internal users.  |
| F | Password Spray |  | O | Procedure that examines multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays and more. |
| N | Phish |  | P | Attach technique that circumvents internet censorship by obfuscating the domain of a HTTPS connection. Working in the application layer, domain fronting allows a user to connect to a service that may otherwise be blocked by DNS, IP or deep packet inspection.  |

**Test Your Cyber Security Incident and Incident Response Skills!**

Match the Term to the correct Description

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Answer** | **Term** |  | **Letter** | **Description** |
|  | Crisis Management |  | **A** | Procedure that treats the internal network as hostile, segmenting different organizational units or systems from each other. Often performed by host-based firewall, iptables, netsh advfirewall tools. |
|  | Isolation |  | **B** | Procedure to baseline a system and verify that is operating in a normal state. |
|  | User and Entity Behavior Analytics (UEBA) |  | **C** | Attack technique using the component of Microsoft **Windows** XP and later iterations of the operating systems, which facilitates asynchronous, prioritized, and throttled **transfer** of files between machines using idle network bandwidth. |
|  | Internal Segmentation |  | **D** | Attack technique that uses the Application Compatibility Toolkit to trick applications into not seeing the ports, directories, files, and services the attackers want to hide. |
|  | Real Intelligence Threat Analytics (RITA) Analysis |  | **E** | Procedure that uses various switch and router commands to quarantine infected system to prevent further harm. |
|  | Firewall Log Review |  | **F** | Brute force attack where the hacker tries to gain access to an organization’s systems by testing out a small number of commonly used passwords on many accounts, on the assumption that within a large group of people, there's likely to be at least one using a common password. |
|  | Server Analysis |  | **G** | Attackers create and load their malware using a service with SYSTEM privileges; or create a new service. |
|  | Domain Fronting |  | **H** | Attackers use a vulnerability in local software to gain administrative access. |
|  | Windows Background Intelligent Transfer Service (BITS) |  | **I** | Procedure that examines the network traffic, parsing and conduct a review.  |
|  | Application Shimming |  | **J** | Procedure by which an organization deals with a disruptive and unexpected event that threatens to harm the organization or its stakeholders. |
|  | Evil Firmware |  | **K** | Valid active directory credentials have been discovered on open shares and files within the environments that are used by attackers. |
|  | Local Privilege Escalation |  | **L** | Attackers update firmware of network cards, video cards, and BIOS or UEFL. |
|  | New Service Creation |  | **M** | Procedure that analyzes firewall logs. Regularly emulate attack scenarios to verify procedures. |
|  | Credential Stuffing |  | **N** | Attackers send a malicious email targeting internal users.  |
|  | Password Spray |  | **O** | Procedure that examines multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays and more. |
|  | Phish |  | **P** | Attach technique that circumvents internet censorship by obfuscating the domain of a HTTPS connection. Working in the application layer, domain fronting allows a user to connect to a service that may otherwise be blocked by DNS, IP or deep packet inspection.  |