**Day 1 Observations - 00:00-23:30 August 20th 2024**

**Summary:**

This is a collection of data from the T-Pot honeytrap I configured to run on a Debian 11 EC2 instance. This first day’s data is from 00:00 August 20th 2024 through 23:30 August 20th 2024 and will be analyzed to provide insights into common attack behaviors, geographic location of attackers, and CVEs exploited. I will then compare the findings from Day 1(August 20th) to Day 6(August 25th) to see the difference in behaviors, geographic locations, and exploits leveraged by attackers.

**The Honeypots of T-Pot:**

* Honeytrap: a honeypot that emulates various types of network services and protocols, such as SSH, Telnet, FTP, HTTP, SMTP, and more. Can be configured to listen on multiple ports and simulate authentic behavior of various services to attract and trap attackers.
* Dionaea: a honeypot that emulates a vulnerable Windows environment designed to capture malware and attack payloads. Uses Python as its scripting language, supports IPv6 and TLS, uses libemu to detect shellcode, and collects hash values of collected files for later analysis.
* Cowire: a SSH and Telnet honeypot designed to emulate a system and provide a shell environment that captures the attacker’s actions on the system. This includes things like tools, techniques, credentials, and commands.
* Redishoneypot: a honeypot designed to emulate Redis servers and databases. Can collect the attacker’s IP address and commands used during connection attempts
* ADB Honeypot: a honeypot designed to emulate an ADB-enabled Android device and log unauthorized access attempts
* Snare/Tanner: a honeypot designed to emulate Windows systems and services that can capture attackers IP addresses, commands issued, tools, techniques, and procedures to identify patterns and send the collected data to security professionals.
* Ciscoasa: a honeypot designed to emulate Cisco Adaptive Security Appliances and software to track attacks targeting Cisco ASA devices.
* Citrix Honeypot: a honeypot designed to emulate a vulnerable Citrix environment.
* Mailoney: a honeypot designed to emulate a vulnerable mail server.
* Conpot: a honeypot designed to emulate SCADA protocols and industrial control systems.
* Elasticpot: this is a honeypot that simulates a vulnerable ElasticSearch server that is open to the internet.
* Dicompot: a honeypot that is designed to simulate a Digital Imaging and Communications in Medicine(DICOM) server.
* Sentrypeer: an open source VoIP fraud detection tool that tracks the IP addresses of attackers making calls to a SIP server.
* Heralding: a simple honeypot that is designed to log credentials of login attempts across multiple protocols.

| Analysis: | Diagram: |
| --- | --- |
| Total amount of attacks registered across the various honeypots that make up T-Pot from 0000 August 20 2024 - 2330 August 20 2024. |  |
| This graph shows the distribution of attacks across the various honeypots. Honeytrap by far being the most attacked followed by Dionaea. From there it is a sharp fall off in the amount of attacks for the remaining honeypots. The attacks are broken down as follows:   * Honeytrap: 51,596 * Dionaea: 22,238 * Cowire: 499 * ConPot: 263 * Tanner: 243 * Mailoney: 165 * CitrixHoneypot: 152 * ADBhoney: 93 * Redishoneypot: 81 * Ciscoasa: 45 * Elasticpot: 37 * Dicompot: 13 * Ipphoney: 9 * Sentrypeer: 3 * Heralding: 1 |  |
| This diagram shows the most commonly attacked ports over time.   * 18080: unofficial but commonly used for Monero cryptocurrency P2P network communications. Sees a steady stream of attacks. * 445: a Microsoft networking port that runs SMB and is linked to NetBIOS in earlier versions of Windows. This is the second most commonly attacked port but is seen in large bursts every few hours. * 37215: This port is used by Huawei routers and is vulnerable to remote code execution. This port saw a steady but low number of attacks. * 7999: This port is used for Microsoft Azure infrastructure communication. This port saw a very low number of attacks. * 8728: This port is used by APIs and also experienced a very low number of attacks. |  |
| This graph shows the number of attacks attributed to specific countries over a period of time.   * The United States shows a consistent high rate of attacks over the whole 24 hour period. * India shows the second highest rate of attacks but this is done in a few high bursts around 0430 to 0630 and then falls off. * Vietnam has the third highest rate of attacks but this is all concentrated in a large spike starting at around 2230. * Indonesia has the fourth highest rate of attacks all concentrated at around 0400. * Canada is the final country with all of its attacks concentrated in a short spike at around 0230 |  |
| This graph shows the top 10 countries based on the percentage of attacks.   * United States: 56% * India: 9% * Vietnam: 6% * Indonesia: 5% * Canada: 5% * Mexico: 5% * Singapore: 5% * The Netherlands: 4% * Lithuania: 4% * United Kingdom: 2% |  |
| This shows the distribution of ports attacked based on the country of origin.   * The United States: most of the attacks focus on port 18080 (99%) * The rest of the countries focused almost all of their attacks on port 445 |  |
| This graph shows the reputation of the source IP of attackers. Most of the attacks are performed by known attackers or mass scanners.   * Known Attackers: 95% * Mass Scanners: 5% * Bot, Crawlers: 1% |  |
| This graph shows the distribution of common OS used by attackers. The three most common being Linux 2.2.x-3.x(66%), Windows 7 or 8(25%), and Linux 2.2.x-3.x barebone(8%). Attackers may choose these older OSs for many reasons from using them to evade detection aimed at more current OSs, environmental factors like limited resources and technical expertise, or known exploits that haven’t been patched. |  |
| This graph shows the categories of the Suricata alerts at different times of day.   * Generic Protocol Command Decode and Misc Attack are the two most common and consistent alerts throughout the whole day * Attempted Administrative Privilege attacks spike at 0030, 2000, and 2300. These attacks attempt to gain administrative privileges and are conducted outside of common office hours to remain unnoticed. |  |
| This is a list of the most commonly attempted usernames to gain access to the instance. The names are usually default names and ones that commonly appear in dictionary attacks. It is important to choose a strong and unique username and to not use the defaults. |  |
| This shows the most commonly attempted passwords to gain access to the instance. The most commonly attempted one was simply no password at all, followed by the common top 10 like password, 12345, root, etc. Much like usernames it's important to choose strong passwords that cannot be easily cracked. |  |
| Top 10 CVEs:   * CVE-2020-11899: this exploit uses the Windows Graphic Device Interface(GDI) and a specially crafted image to allow attackers to execute arbitrary code on the system when the image is opened by the victim. * CVE-2020-2551: this exploit targets Oracle WebLogic Servers versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. This exploit allows attackers to gain unauthorized network access via IIOP to compromised Oracle WebLogic servers and can result in the attacker taking over the server. * CVE-2021-3449: this exploit allows attackers to crash OpenSSL TLS servers by sending a maliciously crafted renegotiation ClientHello message. OpenSSL 1.1.1-1.1.1j versions are affected by this exploit.      * CVE-2019-11500: this exploit affects Dovecot, an open source IMAP and POP3 server for Unix-based systems, versions before 2.2.36.4 and 2.3.x before 2.3.7.2. This exploit can grant out-of-bound writes and remote code execution to attackers because protocol processing can fail for quoted strings because ‘\0’ characters are mishandled. * CVE-2019-12263: Wind River VxWorks 6.9.4 and vx7 has a Buffer Overflow in the TCP component. There is an IPNET security vulnerability where the TCP Urgent Pointer state is confused due to race conditions. * CVE-2002-0013: Vulnerabilities in the SNMPv1 request handling of a large number of SNMP implementations allow remote attackers to cause a denial of service or gain privileges via GetRequest, GetNextRequest, and SetRequest messages. * CVE-2023-46604: This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker to instantiate any class on the classpath. Upgrading both brokers and clients to versions 5.15.16, 5.16.7, 5.17.6, or 5.18.3 will fix this issue. * CVE-2018-11776: Apache Struts, an open source framework for creating Java applications, versions 2.3 to 2.3.34 and 2.5 to 2.5.16 are vulnerable to possible Remote Code Execution when alwaysSelectFullNamespace is set to true which can either be set by the user or a plugin like Convention Plugin. * CVE-2002-1149: The installation procedure for Invision Board, a web forum software that uses PHP, suggests that users install the phpinfo.php program under the web root, which leaks sensitive information such as absolute pathnames, OS information, and PHP settings. * CVE-2019-9621: Zimbra Collaboration Suite before 8.6 patch 13, 8.7.x before 8.7.11 patch 10, and 8.8.x before 8.8.10 patch 7, or 8.8.x before 8.8.11 patch 3 allows Server-Side Request Forgery(SSRF) via the ProxyServlet component. |  |

**Top 10 IP Addresses**

| **IP Address** | **Count** | **City/State** | **Country** | **ISP** |
| --- | --- | --- | --- | --- |
| 162.218.65.219 | 26,480 | Virginia | The United States | Lionlink Networks |
| 14.174.135.196 | 4,150 | Hue | Vietnam | VNPT Corp |
| 180.252.233.195 | 3,149 | Tangerang | Indonesia | PT Telkom Indonesia |
| 189.253.54.138 | 3,149 | Guanajuato | Mexico | Uninet |
| 202.47.166.3 | 3,149 | Kanpur | India | SSN Network Private Ltd |
| 122.176.26.43 | 3,147 | Kolkata | India | Bharti Airtel Ltd |
| 54.39.15.21 | 3,146 | Montreal | Canada | OVH Hosting Inc |
| 119.93.147.253 | 809 | Bohol | Philippines | Philippine Long Distance Telephone Company |
| 171.5.28.30 | 650 | Phuket | Thailand | Triple T Broadband Public Company Ltd |
| 125.26.3.221 | 299 | Pattaya | Thailand | TOT Public Company Ltd |

**Conclusion:**

The first day of this lab gives us a baseline on what to expect for the next few days. The honeypots were subjected to over 75,000 attacks mainly targeting Honeytrap and Dionaea. A majority of these attacks originate in the United States and based on IP analysis we can see that most of these attacks from the US originated in Virginia which is where I hosted the EC2 instance. The next most prolific country is India with only 9% of attacks being attributed to them compared to the 56% perpetrated by the US. The most popular ports were 18080 which is used by the Monero cryptocurrency for P2P network traffic and 445 which is used by Windows for SMB.

The most common operating systems used by attackers were flavors of Linux 2.2.x-3.x accounting for 66% of all OS used, followed by Windows 7 or 8 at 25%, and finally Linux 2.2.x-3.x barebones at 8%. There are many reasons for these operating systems to be used by attackers from technical knowledge, socio-economic factors, or the fact that some of these systems might allow attackers to exploit vulnerabilities that haven’t been patched yet.

The timing of attacks can also give us insight into the attackers such as seeing spikes of attempted privilege escalation happening at 00:30, 20:00, and 23:00 which is outside of regular office hours for most companies in the United States which helps the attackers evade detection. We can also see the attempted usernames and passwords used to attempt this privilege escalation with the most common username being sa, root, or empty; these are all common default usernames. It’s the same for passwords with the most popular being no password at all, admin, 12345, etc which are all common passwords that can be easily cracked via a dictionary attack

The most common CVE utilized was CVE-2020-11899 with 731 attempts recorded. This exploit allows attackers to execute arbitrary code using the Windows GDI. The next three most common CVEs all recorded similar numbers of attacks, first there is CVE-2020-2251 with 17 attempts recorded, this exploit allows attackers to take over vulnerable Oracle WebLogic servers. CVE-2021-3449 recorded 15 attacks and allows attackers to OpenSSL TLS servers. Finally there was CVE-2019-11500 which affects Dovecot and allows attackers to execute arbitrary code if exploited successfully. As we can see two out of the four most popular CVEs result in arbitrary code execution by the attackers.

Overall this gives an interesting look into what attackers are interested in. I’m sure we’ll see continual attempts of privilege escalation and exploits that grant arbitrary code execution throughout the labs runtime. This shows the importance of following network security best practices, such as strong usernames and passwords, strong monitoring compared to a baseline of network activity for the organization, and proactive measures to thwart unauthorized access attempts. Following these best practices organizations can strengthen their networks to prevent successful cyberattacks.