**Observations for August 20th-August 25th 2024**

**Summary:**

This is a collection of data from the T-Pot honeytrap I configured to run on a Debian 11 EC2 instance. This is the culmination of all the data collected over the 6 days that the T-Pot server was up and it will be analyzed to provide insights into common attack behaviors, geographic location of attackers, and CVEs exploited.

**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.

| Total amount of attacks leveraged against the different T-Pot honeypots for the 6 days. |  |
| --- | --- |
| This graph shows the distribution of attacks across the various honeypots. Honeytrap by far being the most attacked followed by Dionaea and Ciscoasa, 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: 305,862 * Dionaea: 92,803 * Ciscoasa: 21,355 * Cowire: 10,094 * Tanner: 3,007 * Mailoney: 1,338 * ConPot: 720 * Redishoneypot: 556 * Citrix Honeypot: 530 * ADBhoney: 254 * ElasticPot: 163 * Dicompot: 90 * Heralding: 85 * Ipphoney: 39 * Sentrypeer: 15 |  |
| This diagram shows the most commonly attacked ports over time.   * 18080: unofficial but commonly used for Monero cryptocurrency P2P network communications. Saw a steady stream of attacks which makes sense because it was the most targeted port by the United States the entire time. * 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 everyday. * 80: a port used for HTTP. Third most attacked port with spikes every day with the largest spike being on August 25th. * 23: a port used for the Telnet protocol. This port experienced a steady number of attacks the entire time much like port 18080 but at a much lower number. * 2323: another port used for Telnet protocol. This port experienced a much more inconsistent amount of attacks compared to port 23 with its largest spike of attacks being seen on August 22nd. |  |
| This graph shows the number of attacks attributed to specific countries over a period of time.   * The United States is clearly the most prolific with a steady stream of almost 5,000 attacks a day for the whole 6 days. * India is the second most prolific with a large spike almost every day, except August 23rd. India also had a large spike of attack numbering around 3,000 for a nearly 24 hour period between August 24th and 25th. * The Netherlands is the third most prolific attacker with a steady number of attacks every day. * Lithuania is a close fourth for most prolific attacker being right behind The Netherlands with a very similar pattern of consistent attacks all 6 days. * Vietnam is the fifth most prolific attacker with the largest single spike of attacks occurring on August 21st reaching nearly 7,000 attacks. From there they had a few spikes on the 22nd and 24th but otherwise launched relatively few attacks. |  |
| This graph shows the top 10 countries based on the percentage of attacks.   * The United States: 66% * India: 9% * The Netherlands, Lithuania, and Vietnam: 4% * The United Kingdom and the United Arab Emirates: 3% * Indonesia, China, and Venezuela: 2%   This graph shows how prolific and consistent the United States was in their attacks, being responsible for 66% of all attacks and the next closest country being India with a mere 9%. |  |
| This shows the distribution of ports attacked based on the country of origin.   * The United States: 99% of all attacks over the 6 days were directed at port 18080(Monero P2P). * India: 100% of attacks were targeted at port 445(SMB). * The Netherlands: 99% of all attacks were targeted at port 18080(Monero P2P) * Lithuania: 99% of all attacks were targeted at port 18080(Monero P2P) * Vietnam: 82% of all attacks targeted port 445(SMB), 10% targeted port 2323(Telnet), and the remaining 8% targeted port 23(Telnet)   In the top 5 countries only Vietnam showed a detectable distribution of ports attacked although the most attacked was the same as India being port 445 and the only unique two ports on the list being ports 2323 and 23 both of which are for Telnet. |  |
| This graph shows the reputation of the source IP of attackers. Most of the attacks are performed by known attackers or mass scanners.   * Known Attacker: 96% * Mass Scanner: 4% |  |
| This graph shows the distribution of common OS used by attackers. The three most common being Linux 2.2.x-3.x(68%), Windows 7 or 8(18%), Linux 2.2.x-3.x barebone(9%), and Windows NT kernel(4%). These have been the four most popular OS for these attacks the whole 6 days showing very minimal changes between the days. 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 is still the most prevalent throughout the whole lab. * The first few days Attempted Administrative Privilege attacks commonly seen either late at night or early in the morning but by the last few days these types of attacks were being seen more during the middle of the work day. This might be because of time zone differences between the target machine in Virgina and the attackers around the world. |  |
| This is a list of the most commonly attempted usernames to gain access to the instance, with the most common during this time period being “sa” and “root” being the most prominent. “Root” was the username of choice the first few days but attackers started using “sa” a lot more the last two days. The names are still common and default names and ones that commonly appear in dictionary attacks or come preconfigured like “pi” or “admin”. 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. 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-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-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-2006-2369: RealVNC 4.1.1, and other products that use RealVNC such as AdderLink IP and Cisco CallManager, allows remote attackers to bypass authentication via a request in which the client specifies an insecure security type such as "Type 1 - None", which is accepted even if it is not offered by the server. * 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-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-2002-1149: 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-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-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. |  |

**Top 10 IP Addresses**

| **IP Address** | **Count** | **City/State** | **Country** | **ISP** |
| --- | --- | --- | --- | --- |
| 162.218.65.219 | 173,101 | Virginia | The United States | Lionlink Networks |
| 80.64.30.188 | 14,285 | Moscow | Russia | Horizon LLC |
| 14.174.135.196 | 11,063 | Hue | Vietnam | VNPT Corp |
| 80.94.95.175 | 6,564 | England | The United Kingdom | UNMANAGED LTD |
| 103.28.33.101 | 3,861 | Da Nang | Vietnam | Viet Digital Technology Liability Company |
| 79.110.62.8 | 3,636 | Amsterdam | The Netherlands | Emanuel Hosting Ltd. |
| 119.226.185.2 | 3,166 | Chennai | India | Sify Limited |
| 103.134.44.223 | 3,153 | Uttarakhand | India | Countrylink Communication Pvt Ltd |
| 190.89.30.131 | 3,153 | Maracay | Venezuela | Corporación Fibex Telecom C.A |
| 132.255.224.74 | 3,151 | Villa Mercedes | Argentina | Sidecom SRL |

**Conclusion**

After running the lab for a week there were a total of 473,324 attacks. Consistently the United States was behind a majority of them, 66% of the total attacks across all 6 days. Honeytrap was the most targeted honeypot with 305,862 total attacks which accounts for 65% of the total attacks. Dioneae was the second most common target with 92,803 attacks recorded which is 20% of the total attacks. Ciscoasa was the third most targeted honeypot with 21,355 attacks recorded which accounted for 5% of attacks.

As far as ports targeted there were two consistently attacked each day. The first, port 18080, which is used by the Monero cryptocurrency for P2P connection was the main target of the United States accounting for 99% of the country's attacks for all 6 days. The second most popular port, port 445, which is used for Server Message Block(SMB) communications was the most common target of most of the other countries that attacked. Ports 23 and 2323 are used by the vulnerable Telnet protocol and it is best practice to close this port and use a more secure protocol like SSH. Port 80 was the final port of the top 5 and is used by the HTTP protocol and being internet facing is commonly attacked. Organizations should use port 443 for their internet traffic to ensure that communications remain encrypted.

96% of the IPs recorded fall under the known attacker or suspicious IP categories, the remaining 4% were labeled as mass scanners. It’s good practice to set up your firewall to block these known attacker’s IPs so they cannot get access to your systems. There are multiple organizations that keep a constantly updating list of malicious IPs such as Project Honeypot or Talos Intelligence. If using AWS they have an option to filter based on an IP reputation list.

CVE-2020-11899 was by far the most commonly used CVE being recorded 4,448 times, compared to the next most used CVE, CVE-2019-11500, only being recorded 102 times. The two most popular types of exploits seen in this lab were arbitrary code execution as seen with CVE-2020-11899, CVE-2019-11500, CVE-2023-46604, and CVE-2018-11776, and denial of service attacks seen with CVE-2021-3449, CVE-2002-0013, CVE-2020-2551, and CVE-2019-12263. The risk of most of these CVEs, especially some of the older ones, can be greatly reduced by upgrading to the latest version of whatever software the exploit is targeting.

As seen in this lab it is important to follow network best practices because attackers are always looking for a way to compromise a system or network. Sometimes simple steps such as using a strong username and password or having scheduled patches to keep systems up to date can keep attackers from getting a foothold into our networks. There are more advanced things we can also do to increase our cyber defense capabilities like, as previously stated, using a list of known malicious IPs and a firewall. Or if a honeypot like this is run and we can see where malicious traffic is coming from we can use techniques like blocking access based on geolocation if we know we have no reason to be exposing our network to a specific region. We should also always make sure to close unused ports and use more secure protocols like SSH over Telnet or HTTPS over HTTP whenever possible.

Overall, this lab has been really enjoyable to run. From getting more hands on experience with AWS to looking at all the data and seeing the trends of attackers it has been a valuable learning experience. Thank you for looking I look forward to doing more projects in the future.