Industry Perspectives on Offensive Security Tooling

Kaitlyn DeValk, Matthew Gwilliam, Thomas Hanson, Michael Harrity, and Michelle Mazurek
University of Maryland, College Park

Abstract

The proliferation and public release of offensive security tooling is a hotly contested topic within the information security industry. Perspectives online vary significantly, and often it seems that the most extreme voices are the ones which garner the highest visibility. We believe it is important to study the general perspectives of professionals within the industry on this topic, not just those with preexisting public platforms. With this aim, we conducted an pilot interview study of eight security professionals to gain novel insight into thoughts and opinions from across the industry. We performed qualitative analysis to distill our results into themes. We used these themes, and our process, to make recommendations for future work surrounding this discourse.

1 Introduction

Offensive security practices like penetration testing are crucial for discovering weak points in a network or piece of software, allowing appropriate patches and mitigations to be implemented. Since routines like penetration testing are critical workflows for many security professionals, many developers have released offensive tools that are open-source and available to the public. In some cases, developers release proof-of-concept exploits to make the public aware of gaps in security defenses, pressure the maintainer to fix the issue, or provide an avenue for testing vulnerability patches. Unfortunately, these tools can also be used by malicious actors.

McLafferty et. al maintain that "offensive security tools can often be defined as the same tools hackers use, but for different purposes. While hackers use these tools for malicious reasons, cyber security professionals use them to find vulnerabilities" [4]. This has created a substantial divide within the community, centering around the public release and proliferation of these offensive security tools (OSTs). Some argue the release of these tools is critical for enabling the work of researchers and professionals throughout the community while others insist that it provides easy out-of-the-box solutions for bad actors, to the detriment of the community [28]. A recent blog even went as far to compare the control of OST release to that of gun control, another highly controversial topic [16]. Seemingly lost in this debate is nuance, and the opinions of everyday professionals are severely under-explored in this space, which provided the motivation for our exploratory study [1].

Within our pilot study, we sought answers to the following research questions:

- **RQ1:** What are the general perspectives in the information security industry on the public release of offensive security tools?
- **RQ2:** What are the ethical concerns that surround these perspectives?
- **RQ3:** How do members of the security industry weigh trade-offs between emboldening adversaries and improving defensive testing?

The interview format gave participants the opportunity to expound upon their answers, which allowed us to collect a rich variety of data. With the perspectives we uncovered, we provide a starting point for future research and best practices regarding the release of OSTs. We performed thematic analysis [13] to distill 11 major themes connected to our three research questions.

2 Background and Related Work

Our study provides a novel look at industry perspectives on OSTs. Here, we discuss existing works that investigate industry perspectives on security topics. Then, we provide some background for discussion on OSTs.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, USA.

2.1 Industry Perspectives

We could not identify a study of industry perspectives of OSTs in the literature. However, researchers have studied the perspectives and practices of cybersecurity professionals extensively for other purposes. Some have performed cognitive task analysis (CTA) to benchmark and understand job performance in a way that would help the authors design better visualization tools [5, 14]. Other works have used interview studies to distill best practices for information security education [9, 11]. Others used interviews [18] and surveys [10] to compare the perspectives of security experts and non-experts on an array of security topics. With each of these, our subject matter is quite different, and our primary commonality is that we are directly querying industry professionals. We also share our methodology in common with the interview studies, and we followed the recommendations of Armstrong et al. where applicable to ensure our studies did not require professionals to compromise key trade secrets or work details [3].

2.2 Prior Work on Offensive Security Tooling

We borrow a provisional definition of offensive security from Anton et. al: "[offensive security], often called red teaming or penetration testing, describes using tools and methods of an attacker to detect security vulnerabilities which then can be fixed before an attacker can exploit them" [2]. Most existing work on OSTs focuses on analyzing the ecosystem, primarily in terms of understanding the tools and actors [2, 6, 15, 19, 20]. By contrast, we intend to gain a better understanding of how professionals view these tools.

Since exploits, once open-sourced, can be used illegally by hackers [25], and the criminalization of OSTs is not feasible due to their importance to legitimate security professionals [26], some prior work focuses on understanding the impact of open-sourcing OSTs. One such work maps modern malware to open source OST libraries in an effort to understand how threat actors are weaponizing OSTs and makes the recommendation to tool authors to "raise the barrier of entry" in limiting the usefulness of a tool while not removing the "tool's educational value" [12]. Another work finds that the public release of OSTs assists with the discovery and subsequent patching of vulnerabilities before malicious actors can exploit them [17].

2.3 Offensive Security Tooling at a Glance

Many different OSTs were discussed over the course of our interviews. To provide background, we briefly describe the specific OSTs we mention in this paper. Shodan is an information gathering tool for internet-connected devices and can identify the protocols and potential vulnerabilities on such devices [24]. The Metasploit Framework (MSF) is a penetration testing platform that provides pre-compiled enumeration, exploitation, and validation modules [21]. MSFVenom is a stand-alone payload generator and is part of MSF mentioned above [23]. Mimikatz is a post-exploitation tool primarily used for exploiting Windows credentials [7]. Powershell Empire is a post-exploitation Command and Control (C2) framework for running modules and evading network detection [22]. Pwncat is a post-exploitation platform for reverse shells on both Linux and Windows operating systems [27]. Hak5 devices are used for physical hacking, such as WiFi pentesting, keystroke logging, or screen [8].

3 Methods

After receiving IRB approval, we conducted semi-structured interviews with 8 participants in order to gain qualitative insight into industry professional's perspectives. Participants were recruited through personal contacts along with snowball sampling as needed. We did not pre-screen since we recruited specific individuals based on their security knowledge and professional experience within the security industry. All participants were U.S. citizens. Brief participant backgrounds and demographics are listed in Table 1. Interviews were conducted via a video call and took 32 minutes on average. Each interview participant was gifted a $10 Starbucks gift card for their participation in the study and was required to give written consent to be recorded during the interviews. In order to refine our research questions and interview process, we conducted a pilot interview with a separate participant whose data is not included in this research.

Table 1: **Participant Demographics.** We show, for each participant, their current area of work, their highest completed education (high school, bachelor's, or master's), whether they have a supervisory role, and their years in the security industry.

P#	Current Area of Work	Education	Supervisor?	Years Experience
P1	Reverse Engineering & Platform Development	BS	No	7
P2	Threat Hunting & Malware Analysis	HS	No	7
P3	Security Architecture	HS	No	11
P4	Offensive Security & Vulnerability Assessments	MS	Yes	8
P5	Digital Forensics & Incident Response	HS	Yes	7
P6	Network Security & Offensive Security	MS	Yes	5
P7	Cybersecurity Engineering & Red Teaming	BS	Yes	6
P8	Defensive Security & Malware Analysis	BS	Yes	4

3.1 Data Collection

Each of our interviews were verbally led by one of two researchers in order to stay consistent. Another researcher was present to take notes, only speaking when clarification was

needed. Our interviews consisted of three parts: a brief section on the interviewee's background, a set on questions about specific OSTs, and a final section on general thoughts surrounding OST release. We used Metasploit and Shodan as baseline tools, and then allowed participants to choose three tools either from personal experience or a given list. The interview script and full set of interview questions can be found in Appendix A. During the interview, we adapted the script with clarification and follow up questions based on the answers from each interviewee.

A recording of the video call was kept to correct mistakes found from the auto-transcription tool used. Following each interview, a researcher listened to the recording and corrected any mistakes in the transcript. Once transcribed, the text was split into question sections for ease of access when coding.

3.2 Qualitative Coding and Thematic Analysis

Due to the size of our study, we only performed qualitative analysis – we did not use any quantitative measures. Since industry perspectives on OSTs are not well-documented in literature, our main goal was to use thematic analysis [13] to identify how security professionals view the public release of OSTs. We used a collaborative coding process to analyze our interviews and accurately identify patterns and trends.

Every interview was independently coded by two researchers, who then met to compare and discuss codes until consensus was met. As interviews were coded, a codebook was developed. Additionally, we kept a running log of all the codes used throughout each interview. This process was continued for all eight of our interviews. Once all interviews were complete, we discussed which codes we thought could be modified by deletion, merging, or separation to maintain a uniform level of specifity across codes. With unanimous consent, we froze our final codebook with 29 different codes, which was done using all 8 interviews. Finally, we had three researchers independently re-code all the interviews using the final codebook without referencing the initial codes assigned. All three coders met and agreed on the codes for each interview, thus completing our collaborative coding and ensuring full consensus. We organize our final codes by themes in Figures 1, 2, and 3 and provide their definitions in Appendix B.

We first analyzed the codes by grouping them based on our research questions and then started to connect themes to the various codes. Collaboratively, we deleted, added, and reorganized themes until each code was related to at least one theme and every theme was considered relevant. During this process, we realized some codes did not answer the research question we initially thought, which caused us to group them differently. We do note that all codes were used for at least one theme across our research questions. At the end of this process, we were left with 11 themes that we felt provided meaningful answers to our 3 research questions.

3.3 Limitations

Our pilot study includes only a small sample, which we recruited based on snowball sampling from a convenience group. This means that we may have missed out on perspectives from outside that group, limiting the generalizability of our results. In this small-sample pilot, we did not reach thematic saturation in our analysis; continuing with further interviews until saturation is reached is an important component of extending this study.

4 Results

We now present the results of our thematic analysis. This section is organized into subsections according to each research question. For each subsection, we provide, in bold font, the themes corresponding to the indicated research question, along with key quotes and analysis for each theme. Figures 1, 2, and 3 show diagrams with our final codes mapped to the eleven themes answering our three research questions.

4.1 General perspectives surrounding public release of OSTs

OSTs have a broad variety of purposes

Our participants suggested several different purposes for OSTs. **P3** described OSTs in terms of their potential uses, specifically their *"capability to audit or assess a weakness against that solution or product."* Others, such as **P1**, reconceptualized OSTs as an educational device, claiming that *"a lot of the places where [powerful OSTs are] actually useful are the learning platforms, places like TryHackMe and HackTheBox and things like that."* **P2** embodied a common refrain; our interviewees tended to define offensive security tooling as *"adversarial based frameworks and programs and applications used to recreate the same tradecraft, tactics, techniques and procedures, that real threat actors and nation-state enemies use in cybersecurity attacks and incidents."*

Anyone can benefit from OSTs

P1 believed that OSTs aid both adversaries and defenders. This view is shared in common across all of our interviewees. For example, **P8** described Metasploit's userbase as containing "white hat or gray hat or black hat hackers." This is connected to the perspective **P4** offers on Powershell (Windows command line tool). **P4** said that Powershell was not designed as an OST, but that, nevertheless, it can be used for offense, regardless of its original purpose. This underscores the notion that any tool can be "misused," and any tool that helps defenders can help attackers as well.

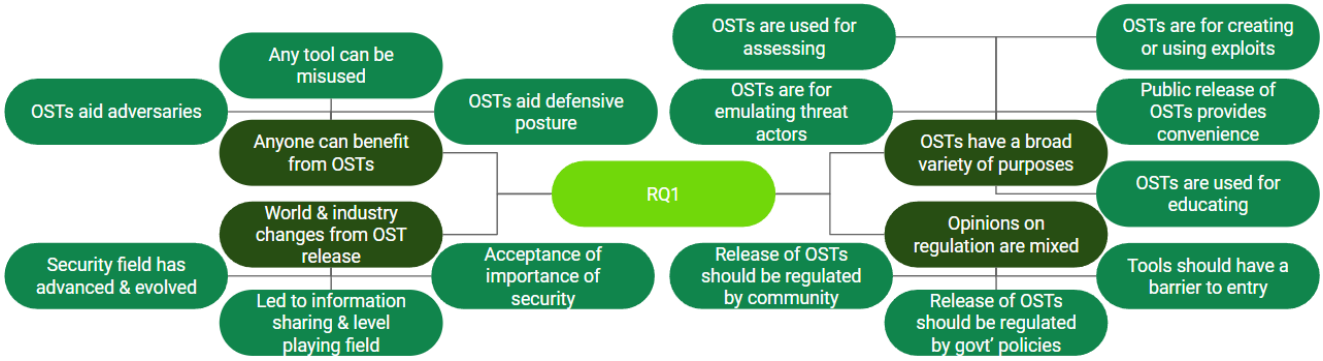

Figure 1: **Theme map for RQ1** (What are the general perspectives in the information security industry on the public release of OST?) Initial connections from the RQ are themes, and secondary connections are the theme-related codes.

World and industry changes have occurred from OST release

Several participants shared **P3**'s belief that OSTs have contributed to the evolution of the cybersecurity field *"and that if we didn't share these sort of tools like [Powershell] Empire or Mimikatz that we wouldn't have grown into this nationwide acceptance of cybersecurity research, as we are now."* Others, like **P5**, offered examples of how OSTs make it easier for decision makers to recognize the importance of security by showcasing, *" 'Hey, this is what a script kiddie can do to your network. You should fix this.' And usually, they'll win over the CFO."* Another common thread was mentioned by **P6** saying that *"at least if [Mimikatz] is public, everyone is equal, there are equal playing field, and you can use it against yourself and test your own defenses."*

Opinons on regulation of OSTs are mixed

Participants were divided on the topic of regulation and OST access. Some agree with the viewpoint expressed by **P5** saying *"I know we're still setting up a lot of major regulatory frameworks in cyber... So, there might be a function that comes out in that soon, but yeah I'd say, let's say, it'd be a positive to have some, some set in stone methods to do that."* Others, such as **P4**, defended the status quo, and claimed that a decentralized framework, such as *"the current ad hoc thing is really cool, because the transparency only helps defenders more."* Within both camps, several people expressed thoughts similar to **P2** who said *"that having a barrier to entry is good,"* or simply decreasing ease of use by removing the "quality of life" features would assist in regulating OSTs without removing their functionality. These notions were in line with recommendations from the previously mentioned study that looked at how malicious actors were weaponizing open source OSTs [12].

4.2 Ethical concerns and considerations

OSTs don't add novel or unique harms

When looking at the ethical concerns participants had surrounding the release of OSTs, some participants didn't believe that OSTs provided any novel or unique harm to people because either the tool was already publicly available and the damage had been done or the capability would inevitably exist anyways. **P1** explained that *"if Shodan didn't exist, people would just be doing it on their own... it's already public information... it's just aggregated in one place and I don't think that's causing any extra harm."*. **P5** had a particularly strong opinion that not having OSTs publicly available *"is asinine because people will figure out how to attack us anyways."* A majority of the participants who held this viewpoint were also strong believers in the open source landscape, and some even mentioned that they have or currently contribute to open source OST projects.

OSTs can cause a variety of harms

As previously discussed, some participants felt OSTs didn't add any unique harms to the landscape. However, other participants specifically mentioned social or physical harm that OSTs could impart on vulnerable populations, such as those in abusive relationships, or lower security-resourced populations, like hospitals or developing countries. **P4** thought of a relationship situation where *"that [Hak5 HDMI replicator] is like a really specific thing, that could be really easy to use and then abused from like, a social perspective... you know the social misuse of that between like normal knowing people... I think that's a scarier use."* **P8** explained a situation where *"the NSA leaked all their all their offensive cybersecurity tools... one of them was like immediately taken and used to execute a bunch of botnet attacks against a lot of American hospitals."* In a similar vein of thought, **P8** also felt that OSTs could make potentially non-technical people feel distressed or confused if they were to see their data exposed. Furthermore,

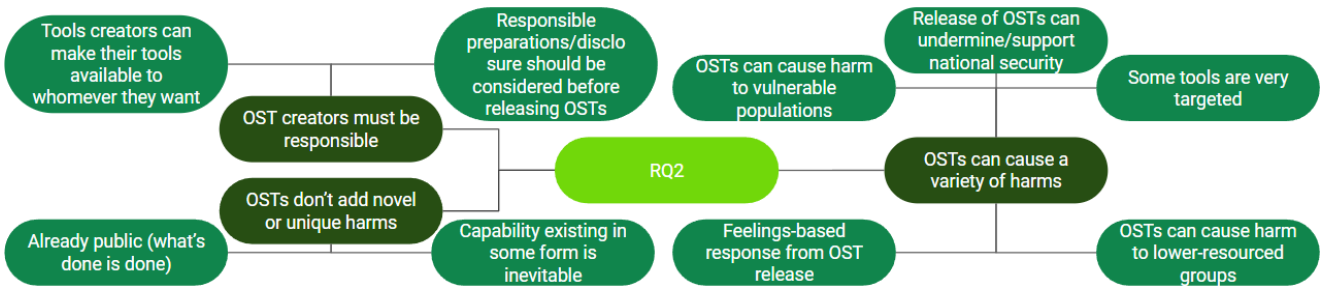

Figure 2: **Theme map for RQ2** (What are the ethical concerns that surround these perspectives?).

several participants brought up the factor of national security in both cases of where OSTs being released have both hurt and helped the government.

OST creators must be responsible

The third theme surrounding ethical concerns that participants had was centered around tool creators, whether it was those who are actively involved in OST development or the responsible treatment and disclosure of vulnerabilities identified in public systems that could lead to the release of an OST. **P2** emphasized the need for imposing required timelines for responsible disclosure and subsequent release of an OST, due to a previous experience where an OST they developed was used to compromise a company's domain during a period of uncertainty about a patch for a particular vulnerability. Other participants felt that notification could mean notifying the affected company or simply making the public aware of the vulnerability without necessarily disclosing the exploit chain.

P4 mentioned a specific ethical concern surrounding commercialized evasion tools where *"... companies may be in a position to provide these obfuscation tools and then you know from their perspective, who and what is ethical to sell to or not and why. And I think that is going to be a really interesting area to think about like ethically."*

4.3 How participants weighed the trade-offs

Accessibility should be changed to balance concerns

Several participants believed that some OSTs, or parts of some OSTs, should not be as easily accessible, whether it was to prevent so-called "script kiddies" from misusing a tool or because the tool was seemingly regarded as purely harmful or dangerous. **P3** thought that Mimikatz was solely a weapon and should not have been open sourced. Another common trend among participants was the mention of including a paywall to increase the barrier of entry or by not releasing targeted or stealthy payloads for frameworks. **P8** stated that *"most tooling in general should be released, but there should be a higher barrier to entry, whether that be like pricing or difficulty of use."*

Trade-off decisions are shaped by personal experiences

This theme shows how our participant's personal experiences have shaped their opinions on OSTs. Many participants offered specific experiences as reasons for why they held a particular belief. This topic is quite subjective, as a participant's specific experiences with an OST are likely to sway their opinion on whether a particular OST or category of OSTs should be released. A couple of these experiences are from **P1**, where *"majority of the use that I've seen out of [Pwncat], and I think where it could really be helpful is people who are learning,"* and **P3** who said *"...from my background, I'm a very huge supporter of just open source in general–us being able to see what's happening is better than us just not having any knowledge of what's possible."*

Security industry is improved in the long term

Another common notion that our participants held was that while OSTs can be used for harm, in the long term, the security industry has and will continue to advance. For example, **P1** felt that these tools being publicly available provides a necessary avenue for companies or security professionals to take a look inward at their own potentially vulnerable systems. Other participants mentioned that sometimes publicly sharing an OST targeted at a particular vulnerability can force irresponsible companies to disclose the vulnerability and hopefully produce a patch.

P3 had a particularly interesting take on how the release of a specific OST forced the evolution of security technology: *"[Mimikatz] gave us the need to develop methods of being able to track its usage, so PowerShell began to evolve at a very rapid rate... Mimikatz for me was really the driver of getting that sort of detection and response just from being able to have improved logging at the technology level."*

OSTs provide harms and benefits dependent on the operator

Our final theme covers the various entities which participants felt were affected by the release of OSTs and who could benefit from these OSTs. The beneficaries included defenders

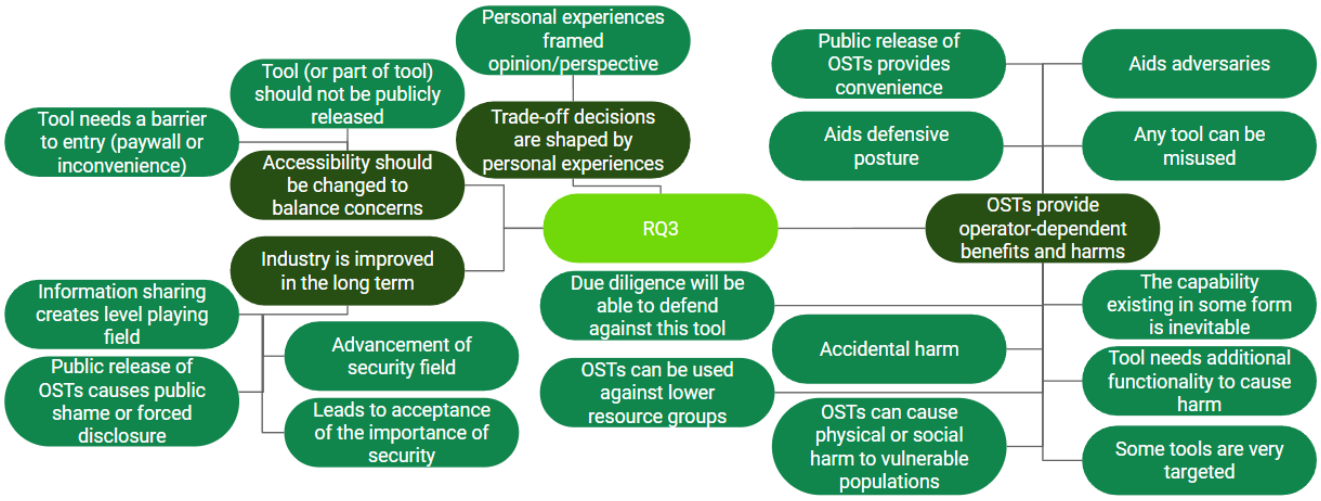

Figure 3: **Theme map for RQ3** (How do members of the security industry weigh trade-offs?).

- **P5:** *"[Shodan] is used in the context of penetration testing. It's used in the context of anybody that's managing OPSEC or operations security general of an organization. So it's kind of useful for everybody..."* - and attackers - **P6:** *"[Metasploit] is a tool, tools can be misused. If you've got a network with holes everywhere, that could potentially be bad. Again, just about any network worth its salt is not under too much danger from it. Yeah, small risk of misuse. Probably worth it in my opinion."* - alike.

P7 also mentioned that while a penetration tester is typically someone whose intent is to advance and support the security of a company, some OSTs make it easy to accidentally cause harm and potentially disrupt business operations such as when *"someone new to the team has decided to put an MSFVenom payload on a mission critical system and not think twice."* These differing viewpoints showcase the intricacies of the OST landscape and that dependent on the situation, the beneficiaries of an OST one day could be victims the next.

5 Future Work

One theme that held potentially actionable findings was "Opinions on regulations of OSTs are mixed," with idea of creating "a barrier to entry." The type of barrier wasn't something well defined within our data, likely due to our sample size, but I think further investigation of this is necessary to see 1) if the community would support implementing barriers for OSTs and 2) what kinds of tools the community thinks warrants a "barrier to entry." Addressing the limitations discussed in Section 3.3 could allow for generalizable themes to emerge regarding information security professional's perspectives on the public release of OSTs. We suggest extending this study with a larger sample of security professionals to gain a wider range of backgrounds. Following this, a survey should be able to provide insight into the proportion of security professionals who agree with each viewpoint, which could inform future policy surrounding OSTs. However, we caution that significant care must be taken to ensure full representation of the industry, and that industry viewpoints may not capture those of all stakeholders, such as organizations with limited security budgets. Finally, we want to study whether there are different viewpoints between those in the public and private sectors. Several participants specifically stated that their respective sector influenced how they answered some questions, but we did not have enough participants to draw convincing conclusions.

6 Conclusion

Our study shows a range of opinions more nuanced than some of the online discussion regarding OSTs. While our sample size was too small to claim these results as representative of all security professionals, we believe that some preliminary lessons can still be learned from our findings. Responsible disclosure is critical, whether it gives developers time to create patches after a bug has been found or administrators time to implement these patches after their release. OSTs can and probably will be used by both defenders and attackers, so developers should consider what they can do to control access to their tools. Releasing an OST prematurely can have negative consequences, but OSTs can also provide an important role in finding flaws and encouraging vendors to fix them. OSTs are also important for education and demonstration, and it bears repeating that the release of a tool is not what creates the vulnerability in the first place. Since there is no hard and fast Industry members disagree on what exactly are the best practices to follow, and further research is needed to establish more comprehensive guidelines moving forward.

References

[1] The call for applied research on offensive security tool release: Chris sanders, Jul 2020.

[2] Simon D Duque Anton, Daniel Fraunholz, and Daniel Schneider. Investigating the ecosystem of offensive information security tools. *arXiv preprint arXiv:2012.08811*, 2020.

[3] Miriam E Armstrong, Keith S Jones, and Akbar Siami Namin. Framework for developing a brief interview to understand cyber defense work: An experience report. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 61, pages 1318–1322. SAGE Publications Sage CA: Los Angeles, CA, 2017.

[4] Michael McLafferty Arthur Salmon, Warun Levesque. Applied Network Security, 2017.

[5] Anita D'Amico and Kirsten Whitley. The real work of computer network defense analysts. In *VizSEC 2007*, pages 19–37. Springer, 2008.

[6] Ajinkya A Farsole, Amurta G Kashikar, and Apurva Zunzunwala. Ethical hacking. *International Journal of Computer Applications*, 1(10):14–20, 2010.

[7] Gentilkiwi. Gentilkiwi/mimikatz: A little tool to play with windows security.

[8] Hak5. Hak5: Our story, 2005.

[9] Julie M Haney and Wayne G Lutters. " it's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 411–425, 2018.

[10] Iulia Ion, Rob Reeder, and Sunny Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pages 327–346, 2015.

[11] Keith S Jones, Akbar Siami Namin, and Miriam E Armstrong. The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education (TOCE)*, 18(3):1–12, 2018.

[12] Paul Litvak. The OST Map: Mapping the use of open-source offensive security libraries in malware, Sep 2020.

[13] Moira Maguire and Brid Delahunt. Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. 8(3):14.

[14] Samuel Mahoney, Emilie Roth, Kristin Steinke, Jonathan Pfautz, Curt Wu, and Mike Farry. A cognitive task analysis for cyber situational awareness. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 54, pages 279–283. Sage Publications Sage CA: Los Angeles, CA, 2010.

[15] Imran Memon, Riaz Ahmed Shaikh, Hadiqua Fazal, Hanif Tunio, and Qasim Ali Arain. The world of hacking: A survey. *University of Sindh Journal of Information and Communication Technology*, 4(1):31–37, 2020.

[16] Daniel Miessler. Comparing offensive security tooling and gun control, Jan 2020.

[17] Valentina Piantadosi, Simone Scalabrino, and Rocco Oliveto. Fixing of security vulnerabilities in open source projects: A case study of apache http server and apache tomcat. In *2019 12th IEEE Conference on Software Testing, Validation and Verification (ICST)*, pages 68–78, 2019.

[18] Clay Posey, Tom L Roberts, Paul Benjamin Lowry, and Ross T Hightower. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & management*, 51(5):551–567, 2014.

[19] Tiffany S Rad. The sword and the shield: Hacking tools as offensive weapons and defensive tools. *Geo. J. Int'l Aff.*, 16:123, 2015.

[20] Nicole Radziwill, Jessica Romano, Diane Shorter, and Morgan Benton. The ethics of hacking: Should it be taught? 12 2015.

[21] Rapid7. Getting started with metasploit for penetration testing. Rapid7 Website (2022/05/08).

[22] BC Security. Empire wiki. BC Security Wiki (2022/05/08).

[23] Offensive Security. Msfvenom - metasploit unleashed. Offensive Security Blog (2022/05/08).

[24] Shodan.io. What is shodan? Shodan Blog (2022/05/08).

[25] B. Smith, William Yurcik, and D. Doss. Ethical hacking: The security justification redux. pages 374 – 379, 02 2002.

[26] Peter Sommer. Criminalising hacking tools. *Digital Investigation*, 3:68–72, 06 2006.

[27] Caleb Stewart. Calebstewart/pwncat: Fancy reverse and bind shell handler.

[28] Andrew Thompson. Misconceptions: Unrestricted release of offensive security tools, Dec 2019.

A Interview Questions

In this appendix, we share our interview script. Since our interviews were semi-structured, we deviated from this script where necessary and appropriate.

Demographics Questions

1. How many years have you been in the security industry?
2. What is your highest education?
3. What area of security do you currently work in?
   (a) What is your job title, and do you have a supervisory role?
4. Have you previously worked in any other areas of security?

Interviewer Specified OST Questions

1. How would you define offensive security tooling?
2. Are you familiar with Metasploit? (Link if need to show participant: https://www.metasploit.com/) Definition/description if participant needs reminder: The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
   (a) Who is Metasploit most useful for? Why?
   (b) Which components of Metasploit should or should not be publicly available? Why?
   (c) What are the benefits of releasing Metasploit? (explain)
   (d) What are the harms of releasing Metasploit? (explain)
3. Are you familiar with Shodan? (Link if need to show participant: https://www.shodan.io/) Definition/description if participant needs reminder: Shodan is a search engine that lets users search for various types of IOT devices (webcams, routers, servers, etc.) connected to the internet using a variety of filters. It can also be used to search for specific vulnerabilities, open ports, or services on these devices. https://www.shodan.io/search?query=mongodb Example showing open ports running mongodb and you can see the vulnerabilities listed along with version info, etc.
   (a) Who is Shodan most useful for? Why?
   (b) Which components of Shodan should or should not be publicly available? Why?
   (c) What are the benefits of releasing Shodan? (explain)
   (d) What are the harms of releasing Shodan? (explain)

Participant Specified OST Questions

Now we are going to repeat the above questions for 3 tools of your choice. Choose one tool at a time and we will ask the questions again. If you need a non-exhaustive list to choose from, we can give examples. (If they can't think of another three, give them a list to choose from: Mimikatz, Cobalt Strike, Powershell Empire, Commando VM/Toolkit, JuicyPotato exploit, Covenant Framework, PrintNightmare exploit, Social Engineering Toolkit (SET), Impacket Framework, Pwncat C2, Nmap)

1. Who is this tool most useful for? Why?
2. Which components of this tool should or should not be publicly available? Why? (whether it is already or not)
3. What are the benefits of releasing this tool? (explain)
4. What are the harms of releasing this tool? (explain)

General OST Questions

1. How do you believe the release of offensive security tools contributes to secure outcomes overall? Why?
2. Do you know of any event where the release of an OST caused negative effects, personally or publicly? Please explain.
3. Do you think there should be a system/methodology in place for releasing offensive security tools? (OPTIONAL depending on time)
4. Where do you draw the line about what types of tooling should or should not be released?
5. What considerations should be taken for releasing a tool exploiting a vulnerability that has not been patched?
   (a) Potential Follow Up (based on their answer): Is it ever acceptable (not acceptable) to do?

B Code Definitions

We provide definitions for all of the codes used in our final codebook. These are the same codes which we use in our theme maps, which we show in Figures 1, 2, and 3.

OST is used for assessing – Participants described this as a way OSTs can be used to identify vulnerabilities, which is meant to help improve the security of a system.

OST for creating/using exploits – Participants said OSTs can be used to develop or use exploits, such as the Metasploit framework.

OST for emulating threat actors – Participants said OSTs can be used to simulate threat actor Tactics, Techniques, and Procedures (TTPs) but this is usually done to test defenders and improve security.

OST is used for education – Participants said that OSTs can help teach people about security as a whole.

Information sharing (creates level playing field, equity) – Participants claimed that if OSTs are made public, then it's a level playing field for attackers and defenders alike; additionally, they felt it cultivated information sharing among the security community.

Leads to acceptance of the importance of security (demonstration of tools) – Participants said that if OSTs are public, they can be used to showcase the importance of security and demonstrate how a bad actor could attack a system or network.

Aids defensive posture – People said OSTs can help defenders because they can be used to showcase security weaknesses.

Aids adversaries (weapons) – Participants gave examples of how OSTs can directly aid adversaries and bad actors.

Already public (what's done is done) – Participants felt that the damage for an already public tool had already been done so there's no point in changing that now.

Advancement of security field (evolution of field as a whole) – Participants felt that the release of certain OSTs helped mature and advance the security industry.

The capability existing in some form is inevitable – Participants felt that restricting the release of OSTs was pointless because someone else would just release it anyways or that the capability would exist eventually.

Tool needs barrier to entry (paywall or ease of use) – Participants felt that some OSTs should have a barrier to entry or restriction of use; one example was very advanced or stealthy implants for C2 frameworks.

Public release of OST provides convenience – Participants felt that OSTs themselves also provided a convenience for some use case usually from their personal experiences.

Release of OSTs should be regulated by the security community – Some participants felt that the way OST release is regulated now, by the security community, should remain.

Release of OSTs should be regulated by government policies/mandates – Some participants felt that public policy or guidelines would help with OST regulation.

Personal experiences framed opinion/perspective – When participants responded at times, they said that their answer was largely based on their personal or professional experiences and sometimes the professional sector they worked in.

Any tool can be misused – Participants made the claim that any tool can become an OST or be misused even if that is not the original intent.

Responsible preparations before releasing OSTs (responsible disclosure project) – Participants felt that responsible disclosure should occur in some fashion before releasing something that could actively harm assets.

Release of OSTs can undermine/support national security – Participants considered national security, saying that certain OSTs shouldn't be released because of national security concerns and that sometimes the release of a tool can actually help improve national security because the OST can now be defended against.

Feelings-based response from OST release – Participants who had an emotional response because they had been personally affected by an OST either positively or negatively.

OST can cause physical or social harm to vulnerable populations (e.g. domestic violence) – Participants stated this as a negative outcome or reason to not release certain OSTs because they could be used against groups who could not as easily defend themselves usually due to lack of knowledge.

Some tools are very targeted – Participants felt that specially-targeted tools should probably not be publicly available or should be behind some kind of barrier usually because they only aid attackers.

OST can be used against lower resource groups (small businesses, developing countries) – Participants stated this as a negative outcome or reason to not release certain OSTs because they could be used against groups usually due to lack of resources.

Tool creators can make their tools available to whomever they want – Participants stated that tool developers have the ability and freedom to make their tools available to whomever they want which can have ethical implications.

Tool (part of tool) should not be publicly released – Participants stated that either an entire tool or a part of a tool should not be publicly released.

Tool needs additional functionality to cause harm – Participants stated that a specific tool alone would need additional functionality to cause harm so they were okay with it being publicly released.

Accidental harm – Participants gave examples where OSTs can be used to cause harm accidentally due to lack of knowledge or inaccurate information provided.

Public release of OST causes public shame or forced disclosure – Participants gave examples where they felt that sometimes an OST should be released to force a company to provide a patch or make a vendor publicly disclose a vulnerability.

Due diligence will be able to defend against this tool – Participants felt that certain OSTs were not harmful because defenses have advanced to the point where it should be easily blocked or detected on a system or network if the company or corporation is implementing proper security measures.