USAID
FROM THE AMERICAN PEOPLE

DEVELOPMENT OF AN OFFENSIVE CYBERSECURITY PROGRAM FOR PROACTIVELY IDENTIFYING AND REMEDIATING VULNERABILITIES

This publication was produced at the request of the the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

MODULE 3 - INTRODUCTION

As any good military strategist or sports enthusiast can attest, the best defense is a good offense. Cybersecurity is no exception to this adage. So let's take a closer look at what Offensive Security is, and how can it help an organization.

At its core, Offensive Security exists to identify issues before they are detected and utilized by external and malicious actors. The term Offensive Security is an umbrella term that covers several aspects of cybersecurity. Let's explore a few of these, in order of the most basic offerings to the most mature.

ASPECTS OF AN OFFENSIVE CYBERSECURITY PROGRAM

1. Vulnerability Scanning

Vulnerability scanning uses automated tools that probe an environment for the presence of known security risks. Though a robust vulnerability scanning program is an essential part of a mature cybersecurity program, such programs rely too heavily on automated scanners and repeatable and scalable processes to function as an Offensive Operations program.

2. Penetration Testing

Like a vulnerability scan, a penetration test, or PenTest, seeks to enumerate risks using a combination of automated tools and human ingenuity. By limiting its scope to a single application or environment, a PenTest can dive much deeper and identify risks likely to be missed by an automated scan.

3. Red Team

The term Red Team is often used interchangeably with PenTesting. While some of their tactics are the same, the two programs have very different strategies and goals. A PenTest is generally time boxed, established on a repeating cadence, with reports generated that are typically delivered to an external entity for compliance purposes. A Red Team engagement, however, can follow any timeline and is often ongoing with a scope as wide as an enterprise. The results are not reported to any external entity. Instead, the Red Team testers take on the tactics of a real-world threat actor to reach the same end goals of that threat actor. Often, that means access, exfiltration, or manipulation of a company's crown jewel assets. These are good guys using the tools and tactics of the bad guys, with permission, to learn what level of risk a company is truly facing.

Such engagements can be carried out with full transparency for the defensive teams, but often they're done with minimal notification so as to test the enterprise's true defensive response to a real attack. Reports generated are only sent internally and serve to identify and provide solutions for proven and executed real-world threats.

4. Threat Hunting

Too many organizations wait to be notified that they've been breached. Yet with the increasing number and scale of cyberattacks—and the sophisticated techniques threat actors are using to mask their activities—the traditional approach of "building bigger fences" will no longer suffice.

The recent hack of Equifax has posed one of the most significant risks to personally sensitive information in years, potentially exposing data for as many as 143 million Americans, according to the report. High-profile, large-scale breaches like the one at Equifax serve as reminders that a defensive cyber approach is no longer sufficient.

In today's unpredictable environment, filled with rapidly evolving threat actors and emerging technologies, the only way organizations can protect themselves is by unleashing offensive cyber techniques to uncover advanced adversaries on their networks. The most effective approach – Threat Hunting—is essential to any organization that wants to stop and prevent attacks in its networks.

Advanced adversaries live in the noise of networks and defeat reactive, rule-based cybersecurity defenses by constantly developing malicious tactics, techniques, and procedures (TTPs). These developments—such as polymorphic and obfuscated malware, dynamic infrastructure, file-less malware, and hijacking legitimate operating system functions—all evade traditional defenses.

During several hunt engagements, many firms find that the time an advanced adversary lies undetected in a victim's network—of 200-250 days before discovery. Threat hunting involves actively searching for compromises before alarm bells go off, carefully combing through networks and datasets to discover hidden threats. By regularly evaluating their networks for threat activity, organizations can catch attacks in progress—before it's too late.

This proactive approach relies on sophisticated tools and tradecraft, such as automation, threat intelligence, threat analytics, and artificial intelligence, to gather and analyze huge reams of data. These tools can identify and mitigate threats at machine speed using customized delivery models.

But not all threats can be detected with automated tools alone. These tools must be paired with trained threat analysts who have a deep understanding of their operating environment and an ability to ask the right questions. Threat analysts can make sense of complex data, develop hunting hypotheses, and test these hypotheses to better identify hidden threats.

Even with trained analysts using the right tools, ad-hoc hunting isn't enough—it must be standardized and measured. Threat hunting requires implementing a repeatable process that's part and parcel of an organization's overarching security strategy. Fusing Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools intelligently can help to streamline this process.

Incidents like the Equifax hack don't have to be inevitable. Organizations need to take steps now to improve their security posture before the next attack hits. Three elements—analytical tools, talented threat analysts, and a standardized hunt process embedded in a broader security strategy—can be the key to knowing your organization is protected.

THE OFFENSIVE APPROACH TO CYBERSECURITY IN GOVERNMENT & PRIVATE INDUSTRY

In recent years, the number of cyber-attacks that hit private companies and government entities has rapidly increased. The damage caused by sabotage and by the theft of intellectual property amounts to several billion dollars each year.

The security community is aware of the growth of cyber threats but the current defensive approach is showing its limit to mitigate the menace from cyberspace. The cyber threats are dynamic and their attacks are asymmetric and difficult to predict.

In the majority of cases victims of attacks can only find losses relating to the raids of the opponents. Law enforcement and private companies are publicly discussing the possibility to define new strategies to defend their assets from the attacks.

The most plausible hypothesis is the adoption of an offensive approach to cyber security, both entities witnesses attended a US Senate Judiciary Committee hearing on proposal of taking the fight to the attackers.

The success of recent attacks conducted by cybercriminals and state-sponsored hackers led security experts to believe that a defensive approach waiting for the attackers it totally inappropriate. In many cases victims discovers the attacks many years, after they occurred when it is too late to apply mitigation measures and the consequences are dramatic.

For this reason law enforcement and private companies are questioning the possibility to adopt offensive techniques to mitigate cyber threats such as, the use of intrusive malware to track the intruders or malicious code to spread in targeted "spear-phishing" campaigns against those actors suspected to have originated the offensives.

Early 2013 the CrowdStrike Company presented its offensive approach to cyber security. The firm revealed details related to the takedown of thousands of nodes of the famous Kelihos botnet. The company is known in the security community because it is exploring all possible legal methods of "*getting stolen information back from hackers, or deleting it definitively avoiding information to be used*".

Stewart A. Baker, partner Steptoe & Johnson LLP, before the Judiciary Committee's Subcommittee on Crime and Terrorism in the paper "*The Attribution Revolution: Raising the Costs for Hackers and Their Customers* " described the actual defensive approach of cybersecurity with following metaphor:

"We are not likely going to defend our way out of this problem"

"In short, we can't defend our way out of this fix, any more than we could solve the problem of street crime by firing our police and making pedestrians buy better body armor every year." "I'm not calling for vigilantism, I'm not calling for lynch mobs. But we need to find a way to give the firms doing these investigations authority to go beyond their network."

"If we don't do that we will never get to the bottom of most of these attacks,"

The hearing before the US Senate Judiciary Committee was also focused on foreign cyber threats, cyber-attacks originated by foreign state-sponsored hackers engaged in sabotage attacks and cyber espionage campaigns represent a serious menace to government security.

How to track foreign hackers? Is a retaliation approach justifiable?

The paper deepens the two parts composing the offensive approach:

- The attribution, the act to search and find clues to track hackers
- The retribution, the persuasion of attackers to choose another policy.

The offensive approach to cyber security isn't a new concept, it has been theorized several years ago and has been debated for a long time, the primary opposition moved against representation by the consideration that it could represent a threat to civil liberties and to user's privacy.

The attribution phase in fact needs a wide range study, to track back hackers it's necessary to make large use for wiretapping activities and also of cyber espionage toolkits, it's clear that both approaches could represent a serious menace for ordinary people and Internet users.

Considering that cyberspace has no physical boundaries, it must be considered that an offensive approach could have consequences on internet users located in foreign states with serious repercussion under legal profile. Recently White House sources revealed to the *New York Times* it was closing a deal that would levy steep fines against any website or internet service, including those based in foreign countries, that refused to support the request of FBI to introduce a built-in wiretapping access within 30 days of receiving a court order.

The debate on offensive cyber security is focused on the possibility to install backdoors and other malicious codes into popular web services and applications to spy on a wide audience of internet users for investigative purposes, a clear violation of citizens' privacy.

Part of the worldwide security community is contrary to the adoption of an offensive approach, Mikko Hypponen, the chief research officer at F-Secure, commented on the use of state-sponsored malware for investigative purposes with these words:

"It's perfectly understandable why law enforcement wants to use malware," "It's an extension to what they've been doing with phone taps, internet taps, and using cell phone carriers to track your location — all with a court order." "However, nothing is as intrusive as having government officials monitoring you through your own computer or smartphone," "They see your files. They see where you surf. They can collect your passwords. They can watch what you do via your webcam."

Despite the approach is not shared by many experts, governments for at least a decade are pursuing an offensive, as invasive, approach to cyber security. Recent surveillance programs such as the US and UK Tempora are the demonstration of government's effort spent in the name of homeland security.

But offensive approach as remarked is not only based on the surveillance program, numerous cyber espionage campaigns are daily conducted by principal governments that recognized the strategic importance to penetrate foreign networks to steal intellectual property and any kind of secret information.

Principal security firms, including Mandiant Intelligence Company, blamed Chinese hackers for numerous cyber-attacks against the US, Mandiant security detailed the clues in an interesting report on the topic in which demonstrated the involvement of Peoples Liberation Army hackers.

Sen. Lindsey Graham on Chinese menace declared:

"Our Chinese friends seem to be hell-bent on stealing anything they can get their hands on here in America," "We're going to put nation-states on notice that if you continue to do this, you'll pay a price."

Rep. Mike Rodgers, known for debated CISPA act, demonstrated skepticism on the possibility to give to private sector offensive conducts.

"I will guarantee you there will be lots of mistakes made, given the sophistication of nation-states in hiding their hand in activities," "I get very, very concerned about an unleashed private sector doing active defense, because a lot of things are gonna go wrong, I think." He declared in February.

THE ATTRIBUTION PHASE MALWARE BASED – JAPANESE CASE

Japan is considered one of the countries most attacked by hackers, government offices and private industry suffered in the past numerous cyber-attacks. Due to this reason the Japanese government has decided to start the development of a software, improperly defined by the press as a "cyber-weapon", which is able to track, identify and mitigate online attacks.

According to The Daily Yomiuri the research on this new type of application is started in 2008, it's an innovative solution, which tries to automatically track and disable the source of cyber threats.

In reality according to government announcements the software is a computer virus developed by Fujitsu for the Japanese government and has the ability to trace cyber-attack sources by reversing the path drawn by the threat in cyberspace. The agent itself infects in fact the various nodes used during the attack and it is able with a high degree of accuracy to localize the origin of offensives such as Distributed Denial-of-Service (DDoS) attacks.

The malware is unique and very innovative according Japan government, it is able to neutralize the attacks and gather a huge quantity of information from the systems abused by attackers, data that could be also used to profile the authors and prevent future attacks. According to security experts, the system in future evolution could also be able to act preventively infecting those systems that have a high probability to be exploited by the same attackers in future offensives.

Commenting on the project, Motohiro Tsuchiya, professor at Keio University and a member of a government panel on information security policy, said Japan should increase "anti-cyberattack weapons development".

The researchers expressly referred the fact Japan isn't the unique state that is working on a similar project, other governments in fact are investing in research for development of a new generation of offensive tools.

The principal question debated on the offensive approach is, that the applications and software could modify the nature of an infected system, abusing their resources if used for an investigative purpose, which is an event that is not accepted by the main security experts.

ZERO-DAYS AS BULLETS

Although in private industry the concept of the offensive approach to cyber security is relatively new, the situation is completely reversed in the government and military environments. Offensive cyber security has long been debated, principal countries have long taken the approach discussed trying by all means to develop systems that can respond if an attack is detected.

One of the principal ingredients for the developments of these solutions are zero-day vulnerabilities, governments driven by the US and China, are principal buyers of zero-day vulnerabilities according to a recent report published by Reuters. The knowledge of a zero-day flaw gives to the attacker a guarantee of success. State-sponsored hackers and cyber criminals consider zero-day exploits a precious resource around which is grown to be a booming market. Zero-day exploits could be used as an essential component for the designing of a cyber-weapon or could be exploited for cyber espionage purposes.

Reuters claimed the US government as the "biggest buyer in a burgeoning gray market where hackers and security firms, sell tools for breaking into computers". The press agency revealed that the US Government, in particular and its intelligence agencies and the DoD are "spending so heavily for information on holes in commercial computer systems, and on exploits taking advantage of them, that they are turning the world of security research on its head.", it's a new way to compete with adversary in cyberspace.

Chinese and U.S. governments have largely invested in the creation of new cyber units, but according to intelligence sources, the offensive approach is considered necessary to preserve the security in cyberspace, recognizing the limits of a defensive approach.

NSA chief General Keith Alexander told Congress that the US Government is spending billions of dollars every year on "cyber defense and constructing increasingly sophisticated cyber weapons" this led to the birth of "more than a dozen offensive cyber units, designed to mount attacks, when necessary, at foreign computer networks."

Charlie Miller, security researcher at Twitter, with a past collaboration with NSA confirmed the offensive approach to cyber security:

"The only people paying are on the offensive side,"

The emerging zero-day market is growing thanks to the intense effort of talented hackers that are exploiting a new way to monetize their knowledge of unknown vulnerabilities especially in large use products.

According to Reuter's defense contractors, intelligence agencies "*spend at least tens of millions of dollars a year just on exploits*", for sure the expense is destined to the new way to interpret cyber security. As declared in the past a zero-day market is very complex due to high "perishability" of the goods, following some key figures of a so complex business:

- ***Difficulty finding buyers and sellers*** – It's a closed market not openly accessible. To find a buyer or identify a possible seller is a critical phase.

- **Checking the buyer reliability** – *The reduced number of reliable brokers able to locate a buyer pushes the researcher to try to tell many individuals about the discovery in an attempt to find a buyer with obvious risks.*

- **Value cannot be demonstrated without loss** – *One of the most fascinating problems a researcher attempting to sell vulnerability information or a zero-day exploit may face, is proving the validity of the information without disclosing the information itself. The only way to prove the validity of the information is to either reveal it or demonstrate it in some fashion. Obviously, revealing the information before the sale is*

undesirable as it leaves the researcher exposed to losing the intellectual property of the information without compensation.

- **Exclusivity of rights** – *The final hurdle involves the idea of the exclusive rights of the information. In order to receive the largest payoffs, the researcher must be willing to sell all rights to the information to the buyer. However, the buyer has no way to protect themselves from the researcher selling the information to numerous parties, or even disclosing the information publicly, after the sale.*

The Current approach to zero-day vulnerabilities is the purchase of exploits, voiding that they could be acquired by government's opponents such as dictators or organized criminals, many security firms sell subscriptions for exploits, guaranteeing a certain number per year.

The Reuters report also revealed the participation of government representatives to the Secret Snoop for Government and law enforcement spying, clearly with the intent to acquire new technologies to conduct cyber espionage through malware based attacks able to compromise target networks.

In many cases the efficiency of these zero-day exploits has a long life, due to the presence of target systems not being updated, typical zero-day attacks have an average duration of 312 days. Once publicly disclosed it is observable in increases of 5 orders of magnitude of the volume of attacks.

Reuters reported to have reviewed a product catalogue from one large contractor, it contained various applications for cyber espionage purposes. The article refers to a product "to turn any iPhone into a room-wide eavesdropping device" and another one "was a system for installing spyware on a printer or other device and moving that malware to a nearby computer via radio waves, even when the machines aren't connected to anything.

In an offensive approach to cyber security the zero-day vulnerabilities are considerable as bullets, their cost depends on a multitude of factors such as the product target, its diffusion level and of course the scope of use. A zero-day sold to a government could have a price up to 100 times that of an exploit kit sold to a private industry.

THE HACKING BANK IN PRIVATE INDUSTRY

Private industry daily suffers attacks from competitors, hacktivists and cyber criminals, since now the principal approach followed is the maintaining of a defensive posture while waiting for government and law enforcement intervention with the hope to track back and hunt down the culprits.

Unfortunately this policy has proved inappropriate to stem a dynamic threat that has increased in intensity and complexity. After the second rejection for CISPA private industry started to think with strength to a more aggressive approach to cyber security.

"It is all well and good to complain about [intellectual property] thefts through diplomatic channels, but at some point you need to stop complaining and start indicting," urged committee chair Sen. Sheldon Whitehouse (D-RI), responding to the affirmation of NSA director general Alexander that defined cybercrime has caused the greatest transfer of wealth and knowledge."

"We are not likely going to defend our way out of this problem," said Stewart Baker, a partner at the law firm Steptoe & Johnson, comparing this approach to deterring street crime by "asking pedestrians to buy better body

armor" every year. "I'm not calling for vigilantism, I'm not calling for lynch mobs. But we need to find a way to give the firms doing these investigations authority to go beyond their network." "If we don't do that we will never get to the bottom of most of these attacks," he said.

Principal countermeasures adoptable by private entities is represented by the use of spyware on a suspected attacker system, exactly as law enforcement does with a court order. The malicious code use is not limited to tracking internet experience, similar agents are used also to infect mobile devices spying on owners. The mobile spying is the last frontier of surveillance. When compromising a device it's possible to track a suspected profile analyzing its surfing activities, accessing to its contacts and massages, listening environment communication through the embedded microphone or accessing to the image captured by camera.

Another option for private companies is try to set up "honeypot" infrastructures to catch the attackers in conjunction with other offensive techniques, such as a "spear-phishing" attack. In this way private firms could try to compromise the attacker's infrastructure with malicious code to recuperate the stolen data or making it unusable.

One of the private industries that demonstrated the highest propensity to an offensive approach to cyber security is entertainment. The entertainment industry is the victim of illegal file sharers that violate copyrights for digital materials. In the eternal fight against piracy the cyber criminals have been staying one step ahead, due to this reason the companies of the sector are evaluating the possibility to attack the pirates with specifically designed tools.

Recently a report issued by the Commission on the Theft of American Intellectual Property, suggested the use of malware as measured security to stop piracy. The document proposed many methods to fight the piracy of copyrighted digital content, including infecting alleged violators' computers with malware that could destroy it. Another possibility is to install a malicious code to track the network of pirates, spying on their activities and recording the abused IP address. In many cases the machines used are not property of the hackers and in other cases the criminals steal IP addresses to use for illegal activities. Monitoring of this information allows the industry to track the crimes and the geographic location of the pirates.

It's known that Chinese hackers are most aggressive persistent collectors, the group that worked on the above report assessing China's role in stealing trade secrets from American companies suggested the adoption of controversial method for defensive purpose … the hacking back of the intruders

"Without damaging the intruder's own network, companies that experience cyber theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information,"

"These attacks [conducted by private companies would raise the cost to IP thieves of their actions, potentially deterring them from undertaking these activities in the first place," "Only when the danger of hacking into a company's network and exfiltration trade secrets exceeds the rewards will such theft be reduced from a threat to a nuisance." States the report.

The need to go beyond the ineffective traditional security countermeasures, such as firewalls and anti-virus software, is pushing the security community to evaluate the "active defense," concept in which private entities break into the hacker's computer and retrieve their stolen files.

Stewart Baker, a former assistant secretary at the Department of Homeland Security remarked the importance to adopt an aggressive approach against foreign hackers, in a blog Baker suggested further methods to persecute the intruders, for example "poisoning" the remote access tools (RATs) that hackers use to exploit computer networks

"It's only a matter of time before counter hacks become possible," Baker wrote. "The real question is whether they'll ever become legal."

During the last edition of RSA Conference chief information security officers (CISOs) and senior security professionals from brand-name companies and government agencies discussed the opportunity to adopt an offensive approach to cyber security. Jeff Bardin, chief intelligence strategist at Treadstone 71 declared:

"Hacker groups and disruption of business have reached an all-time high and no longer can be ignored," "We want to get the adversary to understand that if they launch an attack against a company, there will be costs to pay."

The survey conducted by Wisegate revealed that 40% percent of the IT security leaders interviewed stated that "we should at least be discussing" fighting back; 30% were not ready because "too many legal and ethical questions" are unresolved; and 58% had not even begun discussing a counterstrike policy.

"We need to start thinking like our adversaries, to look at different approaches and techniques to confuse an attacker," "We're looking at using ethical or 'white hat' hackers to check our defenses, and we're approaching our program like we're trying to break into our systems. We need to adopt this mindset and keep focusing on risks." said Wisegate member Tim McCreight, CISO for the Government of Alberta, Canada.

Offensive security tactics have ethical and legal questions, it also must be considered that the economic impact to implement an aggressive approach that is not compatible with the economic condition of the majority of companies.

The approach has an in indisputable collateral effect, whether the victim is or not guilty of piracy, the malware will be installed on his computer with serious consequences. Let's think of a user that has some pirated content on his machine, he may be indicted for piracy and his machine could be destroyed by a legalized counterattack.

The same document discussed notes that "hacking back" could harm the computer system of innocent internet users, let's also consider that hackers use to move the attacks through the compromised computers of unwitting third parties. Still, James Lewis, a senior fellow with the Center for Strategic and International Studies, disagree with the approach because the initiatives of private companies all over the world to hack back the hackers could violate international laws and interfere in relations between states.

"Create the risk that some idiot in a company will make a mistake and cause collateral damage that gets us into a war with China." Lewis said.

The report states that the commission "is not ready to endorse" hacking back because potential for collateral damage or abuse, adding that "further work and research are necessary before moving ahead."

FREE ACTIVE DEFENSE TOOLS INTO THE WILD

Since now Governments and private companies are debating of the offensive approach to cyber security, the jump to the practice is short, a collection of open-source tools is becoming available in the public domain for private companies that decided to persecute intruders.

The "active defense" model is collecting many supporters within private industry and this is pushing a commercial offer that is proposed by specialized vendors such as CrowdStrike, HBGary and Mykonos.

The fundamental of active defense methods includes everything from honeypot-like tools to ensnare potential attackers and to track them. The capability to lure hackers studying their tactics is essential, on the defensive side there are various options, the company could directly attack the alleged criminals that menaces them, or they could choose to limit their active defense interfering with hackers, for example disturbing the attackers' reconnaissance activity and even pinpointing their physical location.

Dmitri Alperovitch, co-founder and CTO at CrowdStrike says that active defense includes activities to real-time detection of threats and identification of malicious agents, deception intelligence dissemination and destruction of attackers' systems as an extreme measure.

"Pure defensive techniques … cannot work when you're dealing with an adversary that's [advanced] and determined to get in, it will find a way in. So you need to find other ways to deter them. That's the premise behind active defense," Alperovitch says.

Another opportunity is to conduct intelligence activities on potential attackers trying to identify their way to act and the targets/information they use to refer. CrowdStrike security firm plans to release various tools for active defense, the company announced the distribution of analyzing and decoding polymorphic malware and free tools to monitor attackers' through Tor.

The market is very prolific, security experts, John Strand, Paul Asadoorian, Ethan Robish, and Benjamin Donnelly, offer a Linux distro set of tools for defense through offense.

ADHD is an active defense distribution with preconfigured strike back tools that could be used to interfere with an attacker's system fingerprinting.

The distro includes defense tools dubbed:

- *Artillery*
- *BearTrap—which opens "trigger" ports on a host to attract the hackers and automatically get spotted and blacklisted.*
- *Decloak to identify the real IP address of a Web user, even one behind a proxy.*
- *Honey Badger to pinpoint the physical location of an Internet user.*
- *Nova (Network Obfuscation and Virtualized Anti-Reconnaissance) detects network-based recon and feeds the attacker phony information on the numbers and types of systems on the targeted network, using*

a network of virtualized decoys. Nova doesn't use signature based detection for malware, instead it creates decoy systems for an attacker to interact with and alert the system administrator for suspicious activities.

- *The Spidertrap is a set of web pages that may intentionally or unintentionally be used to cause a web crawler or search bot to make an infinite number of requests or cause a poorly constructed crawler to crash.*

- *Web Bug Server, embeds a Web bug inside a word processing document that can be used to a hide HTML code that ultimately reveals IP addresses and other information on the attacker.*

"We want to turn the tables without tripping into the realm of hacking back," Strand says. The expert argued legality of such tools sustaining that the offer is addressed to security experts that has clear idea of legal implication of their use. People "ask 'is it legal?' As near as we can tell it is,"

"We cannot go through the steps of getting on their computer or browsing their files even though they are bad guys or criminals. They have a right to privacy, and we try not to cross that line," Strand declared.

READING MATERIAL

1. Module_3_Whitepaper1-7_Secrets_of_Offensive_Security

2. Module_3_Whitepaper2-An-introduction-to-ODS-Strategy-whitepaper