


# Dissecting the NSA's Six-Phase Playbook for Hacking Networks



Think Like the NSA to Keep Your Network Secure

The background of the page features a large, faint watermark of the National Security Agency (NSA) Seal. The seal is circular, with an eagle in the center holding a shield with vertical stripes. The words "NATIONAL SECURITY" are arched across the top, and "UNITED STATES OF AMERICA" is arched across the bottom.

Earlier this year, a 25-year veteran of the National Security Agency (NSA) named Rob Joyce gave a presentation outlining the NSA's six-phase plan for "targeted intrusions" (e.g. hacking a nation state's network). Joyce doesn't go into technical detail or name specific software used by the NSA. His talk is more about the strategic approaches and mindsets that generally work for breaking into theoretically secure networks.

Given that he's the NSA's Chief of Tailored Access Operations (an intentionally obtuse title that means "boss hacker"), these are things he knows plenty about.

There aren't many surprises here if you pay attention to cybersecurity, but you don't often get NSA officials publicly elaborating on the core principals of targeted hacking.

Let's unpack the playbook, and talk about how thinking like the NSA can help us keep our own networks secure.

## Phase One

# Initial Reconnaissance

“Our key to success is to know that network better than the person who set it up.”

“The first phase in a targeted intrusion is the reconnaissance phase. Somebody’s got to go out and know the target... our key to success is to know that network better than the person who set it up.”

*Rob Joyce*

Joyce’s first step is all about knowledge and visibility. Basically, doing your homework on a target to find the cracks in their armor. For any enterprise network, it is likely that there are unauthorized technologies and vulnerable operating systems in use; technologies that users want, but IT hasn’t approved.

This can be anything from vulnerable versions of Apache web server, to cloud

applications (Google Drive, Dropbox), devices (BYOD), password manager apps, and all the other tech that people are actually using on your network that IT doesn’t sanction.


Hackers have a bevy of tools at their disposal to scan your network, identify hosts and operating systems, and probe for vulnerability. You should at least have the capability to detect these scanning methods in action, if not stop them. If a hacker can identify a vulnerable OS, client, database, or other tech handling sensitive data that you don’t have a policy for, you’re already in trouble.

# How to Make Reconnaissance Hard for Hackers

Joyce said the key to the NSA's success is "knowing the target network better than the people who set it up," so the best preventive measure against this phase is to know your network. Consider this: Do you know if there is unencrypted FTP traffic in your environment? How many devices are acting as DNS servers?

The ultimate tip for making the reconnaissance phase tough for hackers is obvious ... yet often overlooked: pay attention.

That doesn't mean "think about it occasionally," it means you need to have systems, technology, and processes in place that give you constant eyes on your valuable data and anyone that touches it. The ability to continuously monitor communication between systems inside your network, often referred to as "east-west" traffic, is a huge part of knowing your network better than any hacker.



“Instrument! Defend! Pay attention to those crown jewels, because that attention and rigor really makes [the hacker’s] job hard.”

- Rob Joyce

## Phase Two

# Initial Exploitation

“All we need is a toehold ... Take these big corporate networks, any large network, I will tell you that persistence and focus will get you in.”

According to Joyce, the importance of zero-day exploits and brand new methods of breaching a network are overexaggerated. He lists three main vectors that hackers use to get the initial toehold they need:

“Most intrusions come down to one of three initial vectors: Email, where a user opened an email, clicked on something they shouldn't have; a website, where they've gotten to a malicious website and they've gone ahead and executed or run content from that website; or removable media, where a user inserted contaminated media ...”

Basically, what Joyce is saying here is that for initial exploitation, they do not need some special, never-before-seen method. Tried and true channels like sending

malware via email still work, because the unfortunate truth is IT security ultimately depends on the end user. So to protect yourself, you need to be paying attention to those channels.

“Most people assume that once security software is installed, they're protected. This isn't the case. It's critical that companies be proactive in thinking about security on a long-term basis.”

*Kevin Mitnick*

Former Hacker and Convicted Felon, Current Computer Security Consultant

# How to Make Initial Exploitation Hard for Hackers

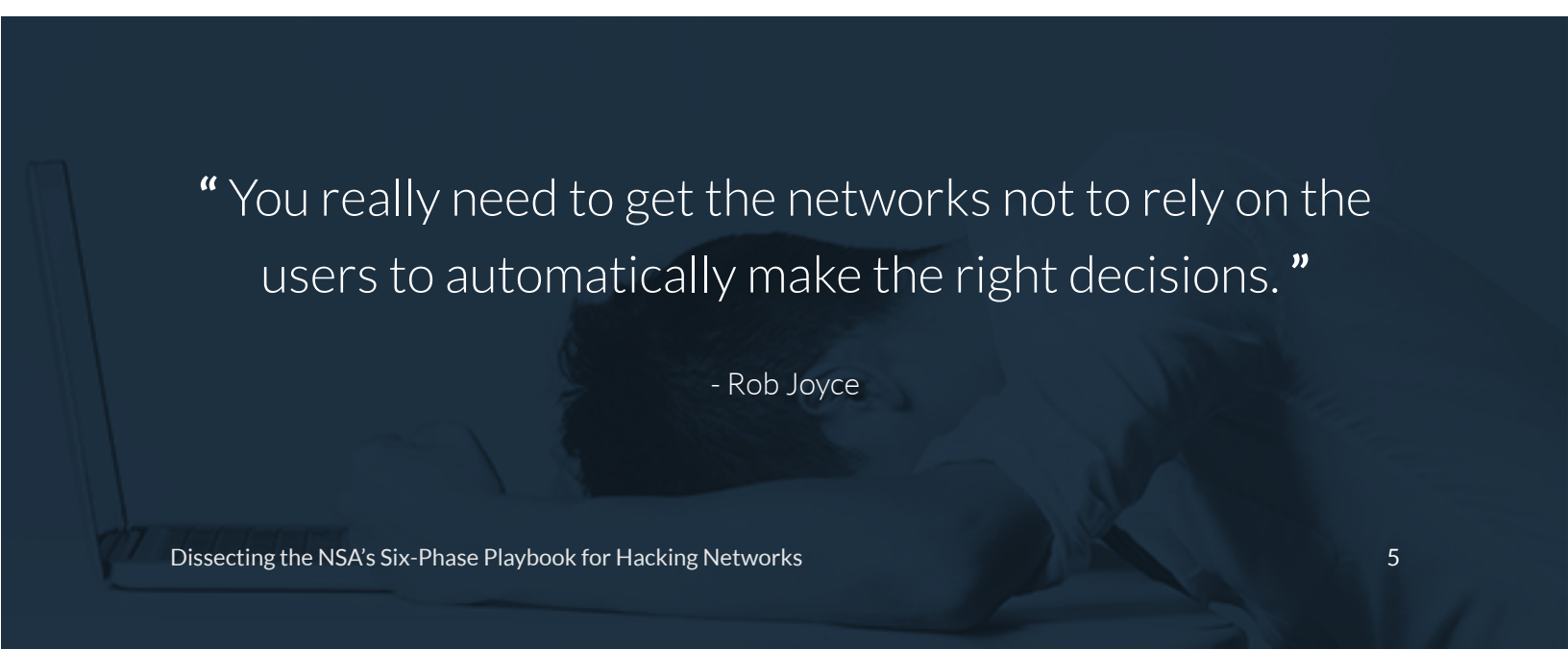
Endpoint protection and antivirus software are essential tools, but they don't protect against social engineering or other methods hackers use to gain control of legitimate credentials.

The [2016 Verizon Data Breach Investigation Report \(DBIR\)](#) found that 63% of breaches involve stolen credentials, and it's much harder to detect nefarious activity being committed with legitimate credentials. You need to be able to [monitor account usage](#), with architecture and policies in place that can mitigate the effects of unstoppable user actions such as clicking on a suspicious link. Google's "[BeyondCorp](#)" [zero-trust architecture](#) is a great example of how architecture and policy can protect you.

This applies to software updates too. If you give your users control over whether or not to update their software when a known vulnerability is closed, you're leaving yourself open to attack.

Monitoring internal traffic and account usage is the best way to both detect user behaviors that put your network at risk, and detect suspicious behavior by user accounts that may have already been compromised.

The key takeaway here is that you need systems in place that keep you secure even if users make bad decisions. Because they will.



“You really need to get the networks not to rely on the users to automatically make the right decisions.”

- Rob Joyce

## Phase Three

# Establish Persistence

“It’s not good enough to just be in a network. If you’re there to exploit, you want to get in and hold.”

Once a hacker is in your network, their goal is to create more backdoors, get a stronger foothold, and generally make it as hard as possible for you to detect them and get them out of there. Persistence can be established by stealing more privileged credentials and malware that can reinstall itself even if removed.

Cybersecurity firm Mandiant [reported](#) that in 2015, the median number of days that hackers had access to a network before being discovered was 146. That number has gone down since 2014, but is still plenty of time to do damage.

## How to Make Persistence Hard for Hackers

This goes right back to Phase 1: Know your network. By understanding what constitutes “normal behavior” on your network for a given user, segment, or functional area, you make it a lot harder for hackers to maintain unauthorized access for long enough to use it without being caught. You need to be able to create baselines founded on continuous monitoring of application and user behavior.

## Phase Four

# Install Tools

“Usually the first tools down are small, lightweight, beaconing things. Their intent is to establish that beachhead and then bring down the tools that are actually going to do the work.”

It is standard procedure for the NSA (and any other attacker) to try to put software on your system that can either exfiltrate data, or force your system to download more software that helps the threat actor become more entrenched.

## How to Make Installing Tools Hard for Hackers

At the time of the presentation, Joyce had two top recommendations for how to stop hackers from installing further tools on your network: whitelisting and reputation services. Here's how they work.

### Whitelisting

This is the inverse of the increasingly ineffective signature-based model of

malware blocking. Rather than blocking known bad software, you make a short list of software that is allowed on your network and block everything else.

### Reputation services

These services check programs against a cloud-hosted database of known executables, to see whether the program is known and whether it has been associated with spam, malware, phishing, or general shady activities. Some reputation services also check domain names that any given software calls out to, so if you see a client calling out to a sketchy domain, you get a warning that it could be malware “phoning home.” If you see a program on your system that a reputation service doesn't like, in Joyce's words: “Be afraid. Be very afraid.”



## Phase Five

# Move Laterally

“After you’re in a network, rarely do you land where you need to be. You need to move laterally to find what you need.”

You have to assume that you will be breached at some point. If you want to be secure, you have to be able to detect suspicious lateral movement in your network. Again, this is also known as east-west traffic. This is the phase where an intrusion goes from a security event that some internal people know about, to a New York Times headline about how your company lost millions of credit card numbers to hackers. With advanced persistent threats, a hacker will get into your network somewhere innocuous and then traverse to a sensitive network share or database.

There’s plenty of room for hackers to mask their misdeeds with east-west traffic. The combined traffic within and between

datacenters will account for 81.8% of all datacenter traffic by 2019 according to the [Cisco Global Cloud Index](#).

“The majority of traffic remains within the data center because of factors such as the functional separation of application servers, storage, and databases, which generates replication, backup, and read and write traffic traversing the data center.”

*Cisco Global Cloud Index*

# How to Make Lateral Movement Hard for Hackers

Continuous visibility into your network, and pre-set policies and controls for allowed activity, are vital for curbing lateral movement. Top strategies include:

## Choose who you trust

Give limited, granular permissions to different users for only the accesses they need. You want a situation where there is no individual user whose compromise could sink your whole operation.

## Segment your network

Along those same lines, don't give everyone administrative access to places where valuable data is stored. Regularly audit and update these access permissions.

## Monitoring and detection inside the network

Assuming you've been breached, do you have what you need to see what the attacker is doing inside your network and make it hard for them to succeed? Monitoring east-west traffic is just as important as monitoring ingress and egress traffic.

## Assign permissions dynamically

Just because a user can access the crown jewels from inside HQ doesn't mean they should also get to access them from a Starbucks across town. A user's access level should be determined, in part, by the security of their connection, their location, and many other factors. Security is not one-size-fits-all.

“Network segmentation, monitoring, caring about your accesses that allow these privileges ... these are all really important pieces ... you really need to limit the administrator privileges, segment the accesses, enforce two-factor authentication. Nothing is more frustrating to us than to be inside a network, know where the thing is we need to get to, and not have a path to get over to find that.”

*Rob Joyce*

Tailored Access Operations  
NSA

## Phase Six

# Collect, Exfil, and Exploit

“At that point, we own you.”

If an attacker is actively exfiltrating data, you're in a bad place but you can't afford to throw up your hands. Things can still get a lot worse from here, and you need to have a plan.

Joyce's take: “Data theft is one arena, but I challenge you to think about another one... what about the [destructive attack](#)? Figure out how you're going to deal with data corruption, data manipulation, or data destruction. It really needs to be something you're figuring out now.”

Not all hackers are trying to make money off of you. Sometimes they just want to hurt you. To see just how bad this can get, [read up on Stuxnet](#), the advanced malware that was allegedly used to destroy Iranian centrifuges by causing them to spin so fast they tore themselves apart.

“Cyber-espionage actors put on their pants the same way we all do. It's just that after their pants are on, they persistently and patiently compromise terabytes of data. In the DBIR, we've seen that the threat actors will start with simpler tools and techniques before moving on to more sophisticated attacks. For this reason, basic protections are still critical to guard against these types of threats, in addition to specialized protection.”

Verizon Data Breach Investigation Report, 2016

# How To Make Exfiltration and Exploitation Hard for Hackers


Let's bang this drum again: visibility, visibility, visibility.

If you can see activity on your network in real time, you can see what the hackers are touching and potentially cut off access before they get all of the “crown jewels,” as Joyce repeatedly calls them. All of the steps before this are directly oriented toward preventing hackers from finding, moving, or destroying data in your system. If you're here, you'd better have a response plan for an extreme data loss event.

Best-case scenario, at least you'll know what you lost and can report it accurately. It looks bad when you disclose a data breach and then immediately have to report that it was [way, way worse than you originally said](#).

Worst-case scenario, you don't even know data is being stolen.

The takeaway here is that you should do everything to avoid getting to this point. Which is obvious, but as the stats show, everyone could do better.



“ 90% of Cyber- espionage breaches capture trade secrets or proprietary information. ”

- Verizon Data Breach Investigation Report, 2016

## Recap

# Visibility Is the Key to Everything

However you feel about the organization, the NSA has some of the best hackers around. When they open up about their best practices, it is worth paying attention. The strongest theme throughout Joyce's talk was that an imbalance of knowledge and visibility in a network is a huge factor in creating vulnerability. Every step of the way, hackers will exploit their ability to see things that you can't in your own network, and will use that lack of knowledge on your part to compromise your security.

If Schoolhouse Rock taught us anything, it is that knowledge is power. Keep up that infosec knowledge by checking out these other great resources:

[Six Reasons your Security Toolset Needs to Include Wire Data](#)

[2016 Verizon Data Breach Investigations Report](#)

[For Ransomware Detection, Behavior Beats Signatures](#)

[Darkreading: How Malware Bypasses our Most Advanced Security Measures](#)

[Learn 4 Ways To Spot A Ransomware Infection On Your Network](#)

[Presentation Outlining the NSA's Six-Phase Plan for "Targeted Intrusions"](#)

“ If you really want to protect your network, you really have to know your network. ”

*Rob Joyce*

Tailored Access Operations  
NSA

# It's Time to Rethink the Network

Visibility into network activity, especially into the fast growing segment of east-west traffic, is the best way to protect yourself from hackers that are using sophisticated techniques like the NSA's. With ExtraHop, you get that visibility with automatic discovery and continuous, real-time monitoring and analytics of all user, device and application activity on your network.

Check out our fully interactive online demo to see what you can do with ExtraHop.



[www.extrahop.com/demo](http://www.extrahop.com/demo)

## About ExtraHop

ExtraHop makes real-time data-driven IT operations possible. By harnessing the power of wire data in real time, network, application, security, and business teams make faster, more accurate decisions that optimize performance and minimize risk. Hundreds of organizations, including Fortune 500 companies such as Sony, Lockheed Martin, Microsoft, Adobe, and Google, start with ExtraHop to discover, observe, analyze, and intelligently act on all data in flight on-premises and in the cloud. To experience the power of ExtraHop, explore our interactive online demo. Connect with us on [Twitter](#), [LinkedIn](#), and [Facebook](#).

