

Intelligence Preparation of The Battlefield

Doug Fordham 2000-06-19

Introduction

"Intelligence Preparation of the Battlefield" is a term used in the military that defines the methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. It is a continuous process that is used throughout all planned and executed operations. The networked environment which security professionals are tasked with securing is analogous to a battlefield. The myriad of attackers and intruders from the void are the aggressors constantly on the offense. The security professionals are the defenders, entrusted to preserve the confidentiality and integrity of data against these marauders.

Recent efforts focused on assessment of critical systems and infrastructures have turned-up a recurring theme. Specifically, that many system and security administrators are unaware of the level of effort that a determined attacker who is well financed and supported will expend towards successful penetration of a target system or site. Most assume that the major threat will come from "script kiddies", and others, who are simply looking for a soft target, and who will move on to easier targets if the initial attempt at compromise is unsuccessful. While this assumption may be true, consideration should also be given to the concept that an attack may be planned and coordinated to a high degree with the specific intent of breaching the target system no matter the cost or effort required.

Security professionals are expected to have a high level of technical competence, and for the most part this is true. However, these same professionals oft times do not expect the same to be true of those attackers and intruders from whom they defend their sites. Many do not take heed of the axiom that "There's always someone out there smarter, more knowledgeable, or better-equipped than you."

Setting The Scenario

Let's assume that the opposition is well financed and supported, and that their technical expertise is on par with that associated with experienced and well-seasoned security administrators. How might this individual, or possibly attack cell, prepare for a successful penetration of a target system? What are the objectives, methodology, techniques and tools utilized? The following seeks to address the above questions, and extend to those tasked with

security related responsibilities an appreciation for the extent and level of effort that, in some cases, may be directed against systems for which they are responsible. It can also serve as a template for an assessment conducted as a preemptive security measure.

The First Steps

The attacker will begin by defining an end-state with regard to the targeted site or systems. This end-state is a clearly defined and obtainable objective. Detailed concepts for courses of action will be formulated and the chosen course of action will concentrate overwhelming "force of effort" at the critical service or vulnerability at the appropriate time and place to achieve the desired effect. Desired results may be denial of service, acquisition of sensitive corporate data, or to establish and maintain access for recurring clandestine access.

Preparation for a successful attack embodies a systematic approach to exploitation. Such an approach fosters effective analysis by enhancing application of professional knowledge, logic and judgment. The attacker will seek to identify and define problems associated with breaching the target defenses, gather facts and make assumptions, develop possible courses of action, and analyze each course of action through "wargaming". Finally, the attacker will choose the best solution available based on the defined end-state and implement the attack.

Estimate of the Situation

In order to develop a coherent strategy, the attacker will complete a thorough estimate of the situation. He will seek to gain a deeper understanding of the task at hand. A review of known facts and information will be conducted. Specific tasks that must be accomplished will be drawn up, and from this task list a reduced essential task list will be constructed. A determination of all constraints and limitations which may influence task accomplishment will be made. How much time is available, location restrictions - can the target system be accessed from the attacker's current location if outside the physical borders of the country the target is located in, or must he move to closer proximity etc. - the materials required in terms of software and hardware, and the associated cost. The attacker will also determine the acceptable risk. Can he afford to be logged during scanning, is compromise acceptable during the latter stages of the attack, is concealment of the originating attack location necessary, and what about exposure of the sponsor if he is working on the behalf of another entity? Finally, any critical facts and assumptions not covered previously will be addressed, and a continuous time analysis maintained until the attack is complete.

Intelligence Preparation of the Battlefield

How will the attacker accomplish the tasks that have been outlined? By laying out a focused plan for acquisition of critical information required for successful penetration of the target system. The following methodology is an example. Most, if not all, of these steps will be executed:

- Define the Network Environment
- FootPrinting
- Scanning
- Enumeration
- Vulnerability Mapping
- Attack Strategy Development & Wargaming
- Refinement & Implementation of the Attack

Define The Network Environment

Defining the network environment involves footprinting, scanning, and enumeration.

FootPrinting allows the attacker to limit the scope of his activities to those systems that are potentially the most lucrative from an vulnerability perspective. Scanning will tell the attacker what ports are open, and services that are running. Enumeration is the extraction of valid account information and exported resources.

FootPrinting

During the footprinting subset of defining the network environment, the attacker's objective is to gather the following information:

- Name and IP of select systems
- Hardware and operating system (including version/build) of the system
- Services available on the system
- Physical location of the system(s)
- Information on individuals associated with the system(s); name, phone #, position, address, knowledgeability etc.
- Build a simple network map for the domain, including connectivity provider and key

systems

- Develop any information that may make it easier to conduct "social engineering"

The methodology to accomplish footprinting of the target will involve non-intrusive and stand-off methods. The attacker wants to determine the type of network with which he is dealing, and with whom; system, network, and security administrators. His tactics and techniques will usually involve the following:

- Check for a website associated with the target. Many websites provide a revealing amount of information that can be used in the attack. Other items of interest include: related companies or entities, merger or acquisition news, phone numbers, contact names and email addresses, privacy or security policies indicating the type of security mechanisms in place, links to other web servers related to the organization.
- Gather information that could be used for social engineering, identity of network systems, system administrators etc. USENET and WEB searches on the system administrators and technical contacts that are found when running host queries. By taking the time to run down this information, the attacker may be able to gain greater insight into the target network. He will also try the system administrator's address on any other machines, if found, when running the host query. Perhaps the system administrator favors one certain machine which can be more readily exploited.

Tools and procedures used to accomplish the task of footprinting:

- Conduct Open Source information gathering on USENET, search engines, Edgar database etc.
- Execute a whois query using the following:

<http://www.networksolutions.com/> - whois web interface

<http://www.arin.net/> - whois ARIN Whois

<http://whois.ripe.net/> - European Whois

<http://whois.apnic.net/> - Asia Pacific IP Address Allocations

<http://whois.nic.mil/> - US Military

<http://whois.nic.gov/> - US Government

or use the native UNIX whois from the command line:

```
whois |more
```

`whois` to gather information on SYSADMIN etc.

Again, the intent is to develop a network map using information gathered during footprinting. The attacker will also want to know who the target gets their upline Internet access from. In the event that he cannot exploit the specified target, he may be able to step back one hop to the service provider for the target and gain access from that vantage point. Additionally, he will figure out which systems are routers and firewalls and place them on the map, as well as identifying key systems such as mail servers, domain name servers, file servers etc.

Scanning & Enumeration

At this point the attacker has a good idea of the machines on the network, their operating systems, who the system administrators are, and any discussions by them as to the topology, policies, management, and administration of their systems posted to newsgroups and other public lists. He also knows that from this point forward everything he does may be logged, and at a minimum will assume it is.

The attacker is now ready to move on to actual reconnaissance of the target, scanning and enumeration. His objectives after the initial assessment of the target system(s) focuses on identifying listening services and open ports. Once promising avenues of entry are identified, more intrusive probing can begin as valid user accounts and poorly protected resource shares are enumerated. The techniques, tools and procedures will vary according to his level of expertise and ability to code custom scripts and programs. Regardless, there is a plethora of open source tools available for use, and he will more than likely make use of some, if not all of the following: NMAP, STROBE, NESSUS and SATAN variants SARA and SAINT if using Linux; WinScan, Sam Spade and others if using a Windows box. Do not discount the fact that commercial products such as CyberCop Scanner and Internet Security Scanner may be used also, as these are available for sale on the open market.

The attacker knows that there is really no good time to ever implement a scan, and that once the decision is made to execute the scan, that it should be done only once. He knows that he may get only one chance, and that another opportunity may not be presented as running a scanner is the equivalent of running up to an occupied building with a crowbar in broad daylight and trying all the doors and windows. He will avoid these types of scans to the maximum extent possible.

The attacker will also make use of tools available as part of the operating system originating the scan and enumeration such as the following for Unix systems:

- `host -l -a |more`
- `nslookup -query=HINFO`
- `dig`
- `dig -x` Do a reverse dig on a couple of systems found when running the host command to see if they are properly reversed mapped
- `dig@ version.bind chaos txt |more` (Used to find out if a vulnerable version of "bind" is being run on each of the domain name servers.)
- `rpcinfo -p` (Used to identify vulnerable or unnecessary RPC services like SPRAYD, STATD, BIOD and WALLD)

Vulnerability Mapping

Once the preceding has been accomplished, the attacker will study and analyze all the information that has been collected. Vulnerability mapping is conducted to match specific exploits to the target systems found during the previous stages. Public sources such as BugTraq and CERT advisories are consulted, public exploit code is reviewed, as well as the output from scanners such as CyberCop, Nesssus and SAINT. If he is not intimately familiar with the operating systems in use, additional study will be conducted prior to gathering the tools required for actually breaching the target.

As a last step to vulnerability mapping, the attacker will gather potential tools for use against the system(s) based on the analysis of the services running, operating system, and other variables. Additionally, evaluation of selected tools to determine what areas they cover is conducted to identify any gaps that may exist in the required capabilities.

Wargaming

The attacker now moves into the final stage before actually conducting the attack, "Attack Strategy Development & Wargaming". The attacker will develop multiple courses of action (COA) and wargame them, selecting the best COA based on all available information. The plan of attack will depend on what is to be accomplished; compromise of security, access, denial of service etc. The attacker will conduct rehearsals, laying out how the attack will be accomplished and working through the exploitation process at least mentally. If possible, he will establish a

single machine with the identical distribution as the target and run a series of attacks against it. The intent here is to identify what the attacks are going to look like from the attacking side, and what the attacks will look like from the victim's side. He will also consider the following influencing factors:

- How stealthy does he need to be?
- Does he need root level access to attain his goals?
- Does he want to attain access to other machines? (Deploy sniffers, get passwd files etc.)
- Which exploits are most likely to succeed?
- Will he want to maintain access to the target system, or is this a one crack deal?

The attacker will seek to be totally prepared before any exploits are run. He will not want to be in the position of acquiring access, and then realize that he does not have a log wiper or a sniffer that is required to further his aims. He will also be prepared with strategic backup plans. For example, if the target system doesn't have a compiler, and he needs to compile tools on the system, he will have a compatible compiler ready to FTP to the target site; or have tools pre-compiled for the target operating system. He will adhere to the maxim "FAILING TO PREPARE IS PREPARING TO FAIL!!"

Attack Implementation

Once all is in preparedness, and at the appropriate time based on reconnaissance and analysis of all data, the attack will be initiated. The objectives are to gain access and to subsequently achieve any of the following: escalate privileges, pilfering, create backdoors, covering tracks, and if all else fails and the attacker cannot achieve his goals, possible denial of service attacks. The attacker will execute the identified exploit in an attempt to gain access. If access is gained, and no system administrators are on the system, and if only user level access was gained in the last step, an attempt is now made to gain control of the system through ROOT/ADMINISTRATOR privileges. This can be conducted using password cracking tools and exploits such as Crack 5.0a, LOPHTCrack, rdist, getadmin, sechole , and buffer overflow exploits etc. Onsite system tools will be used as well as tools imported to system.

Assuming ROOT/ADMINISTRATOR privileges have been gained, the attacker will seek to identify mechanisms to access "Trusted Systems" by evaluating trusts, and searching for cleartext passwords etc. Tools and techniques used can include searching for .rhosts files in users home directories and elsewhere, gathering user data, and examining system configuration files.

Once ownership of the target is accomplished, this fact needs to be hidden from the system administrator. For a Unix based system, the attacker will unset the history file, and execute a log wiper to clean entries from UTMP, WTMP, and Lastlog. For Windows based systems, event log and registry entries will be cleared/cleaned.

If the attacker wants to maintain access to the system after initial access is achieved, he will set about creating backdoors for future access. The methodology, tools and techniques are system dependent, but the intent is to create accounts, schedule batch/cron jobs, infect startup files, enable remote control services/software, replace legitimate applications and services with trojans. Possible tools include: netcat, VNC, keystroke loggers, adding items to the Windows startup folder or configuration files (system.ini, win.ini, autoexec.bat, config.sys etc.) For UNIX based systems, entries in the /etc/rc.d directory can be employed.

If all else fails, or if the desired intent is to implement a denial of service (DoS) attack, the intruder will use exploit code to disable target. This is system/operating system specific and can also depend upon the "patch level" of the system state. SYN flood, ICMP techniques, overlapping fragments/offset bugs, and out of bounds options can be employed. Again, the effect will depend in large part on the system state. Has the system administrator installed the current security package and updated the system files to preclude the implementation of the Ping of Death, Smurf, Fraggle, teardrop, boink, and newtear exploits? The attacker knows that once exploits become public, they can quickly become useless against systems where the system administrators are on top of things, but he also knows that new exploits are found daily and that research and experimentation is required to find the most effective tool and technique.

Post Attack Review

Whether or not the attack was successful, the attacker will conduct an extensive review of his efforts. The intent is to identify what worked and what did not and why. What methodologies were successfully employed, what tools and techniques were most effective and why? This information is paramount if the attacker has to step back through any of the preceding steps along the way to accomplish his intended objective, and for use against future targets.

Conclusion

Finally, the dedicated attack is not the work of a "script kiddie", or casual system intruder. The

opponent that system and security administrators face in this instance is a professional antagonist whose skills may match or exceed their own. As Seth Ross notes in his book *Unix System Security Tools*: "There are no Turnkey Security Solutions. If computer security is a game, then the enemy makes the rules".

Whether working for himself or some other sponsor, we can be sure that the dedicated attacker will adhere to the following:

"There is no way to become either a master system administrator or a master cracker overnight. The hard truth is this: You may spend weeks studying source code, vulnerabilities, a particular operating system, or other information before you truly understand the nature of an attack and what can be culled from it. Those are the breaks. There is no substitute for experience, nor is there a substitute for perseverance or patience. If you lack any of these attributes, forget it!! " (Maximum Security, A Hacker's Guide to Protecting Your Internet Site and Network by Anonymous)

We would be wise to heed these words as well...

Doug Fordham is a former Department of Defense, Information Systems Security Project Manager whose responsibilities included computer network defense, security auditing, and vulnerability testing.

Relevant Links

[Managing Network Security: Anatomy of a Successful Sophisticated Attack](#)

Fred Cohen

[The Structure of Intrusion and Intrusion Detection](#)

Fred Cohen

[Privacy Statement](#)

Copyright 2006, SecurityFocus