BACKTRACK IN THE OUTBACK - A PRELIMINARY REPORT ON A CYBER SECURITY EVALUATION OF ORGANISATIONS IN WESTERN AUSTRALIA

Craig Valli, Andrew Woodward and Peter Hannay
secau – Security Research Centre
Edith Cowan University
Perth Western Australia

ABSTRACT

The authors were involved in extensive vulnerability assessment and penetration testing of over 15 large organisations across various industry sectors in the Perth CBD. The actual live testing involved a team of five people for approximately a four week period, and was black box testing. The scanning consisted of running network and web vulnerability tools, and in a few cases, exploiting vulnerability to establish validity of the tools. The tools were run in aggressive mode with no attempt made to deceive or avoid detection by IDS/IPS or firewalls. The aim of the testing was to determine firstly whether these organisations were able to detect such hostile scanning, and secondly to gauge their response. This paper does not extensively analyse the resultant empirical data from the tests this will be the subject of several other papers.

Of the 15 agencies investigated, only two were able to detect the activity, and only one of these escalated this to authorities. Many had intrusion detection or prevention systems, but these did not appear to detect the scanning which was conducted. Others did not have any form of detection, only logging without active monitoring and some had no persistent logging of anything. Of those who did detect, the lack of a formal incident response and escalation plan hampered their ability to respond and escalate appropriately. Many of these organisations had recently, or very recently undergone penetration testing by external audit or IT companies, and yet there were still numerous vulnerabilities, or their system did not detect the scan. The conclusion is that organisations need to be very specific about what their needs are when engaging external agents to conduct network security testing, as current penetration testing is giving them a false sense of security

1. INTRODUCTION

This paper examines issues uncovered as a result of vulnerability assessment of information systems across 15 large organisations across various industry sectors in Perth, Western Australia. This assessment involved a team of 5 staff for a period of 3 months. There was a variety of assessments performed including documentation and policy review as well as live enumeration and penetration testing of systems over an extended period of time. The NIST SP800-115 document defines penetration testing as attempting to break in to a system (Scarfone *et al*, 2008). The reality is that most audit firms who conduct penetration testing are really only performing vulnerability scanning. This is not to be confused with vulnerability assessment, a process which examines overall security posture of an organisation, and examines network configuration, policy, procedure, compliance, governance and change management, which are all often causes of any vulnerability found by scanning. An appropriate analogy would be that vulnerability identifies the symptoms of security issues, whereas vulnerability assessment finds the cause of the disease. As such, treating the symptoms found by a vulnerability scanner is analogous to taking a pain killer to treat a sore throat, whereas a vulnerability assessment would determine that antibiotics are needed to treat the cause of the infection.

This paper will focus on issues surrounding the penetration testing of the systems and issues uncovered in this process.. The organisations were told that their systems were going to be tested and that they should use normal escalation procedures should they detect an attack or compromise of a

system. The organisations were not told the nature of the testing nor its duration, magnitude or frequency, they were told simply when testing would start. At the conclusion of the testing period organisations were given an exit interview to give feedback but also to check how well if at all detection of attacks had occurred and what if any action had been taken. This paper outlines some of the macro issues and errors that are still being perpetrated by organisations.

2. THE RULES OF ENGAGEMENT

The main idea or thrust behind the penetration testing was to enumerate and attack information systems used by the organisation for service delivery. This focus encompassed not only conventional email and web systems but also VPNs, video conferencing systems and a variety of bespoke systems that had external IP. The other primary directive was that there was to be no specialised attacks or advanced enumeration techniques used in the conduct of the testing. This meant attacks had to resemble those that could be mounted by novice users who downloaded freely available tools and used online information sources to educate themselves and perpertrate any malfeasance. An example of this was the web testing tool nikto (Sullo & Lodge, 2011) that was used in default modes no IDS/IPS evasion techniques were utilised. Nmap (Fyodor, 2002) similarly was used with the nmapfe frontend and selections of options were taken from these default menus to perform port scanning, service identification and operating system.

The attack intensity also escalated in magnitude as the testing progressed for example initial enumeration was done doing scans that probed every 15 seconds to highly aggressive all ports all service scans that emanated 50-100Mbytes of traffic, across entire B Class address spaces in 5-20 minutes. Likewise, password brute force attempts initially at low connection rates ~ 1 attempt every 5 secs to literally the complete set of dictionaries on the Openwall CD exhausted as quickly as the tool or the connection could carry them. The latter with even basic bandwidth monitoring would have detected.

The attack platforms were that of a home user ADSL account supplemented by cheap cloud based virtual servers for instance no server used cost more than $70 for a years subscription and had a bandwidth limit of 1TB of traffic a month. It should be noted that the servers were on fast high speed links and were capable of delivering sustained attacks of large volume.

There were 3 people conducting probing of the 15 targets from a total pool of 12 real IP addresses. The attacks were consistently from these IPs across the 15 targets, however timing was such that any co-ordination of the attacking IPs would have been coincidental beyond each attackers set of IPs. As to escalation the relevant authorities were aware of the testing period and the attacking IPs.

3. TOOLS USED

The tools used were freely available and well known attack tools they were primarily sourced from BackTrack 4 CDs on local laptops. The virtual servers all used Ubuntu 10.10 default installs as the base system that was supplemented with commonly used binaries for security testing and penetration such as nmap, nikto and others.

For enumeration principally nmap was used for service and system enumerations, this was supplemented by the use of httprint and nikto or other specific tools as needed when enumerating or fingerprinting services. As previously mentioned this tools utilised nothing other than default options available in menus, to reflect the reality of a relative computer novice.

For system wide attack again default tools were used perpertrate attacks against identified services or operating system platforms, these included nessus and metaploit. The approach with attack was an increase in magnitude initial attack profile was attack against an enumerated service for instance running a SQL injector against an identified SQL server again using default or noisy methods. This type of attack would not be specific for instance if the scan reported a SQL server on a Microsoft platform an SQL tool that attacked other platforms was utilised as well meaning that any even poorly

configured IDS should have detected a series of attacks.

Having attempted lower magnitude attacks these then were systematically escalated to full noise indiscriminate brute force attacks. An example is metasploit autopwn was used against a host with impunity and basic limitation was bandwidth of connection to carry the attack, no evasion, no tweaks.

The final stage of attack was that of social engineering using USB memory sticks as the vector that was simply dropped or left within the business building perimeter. The USB vector was not designed to autoboot and activate at insertion of the drive. The USB had 3 files on it namely a readme.txt, a modified binary called encryptor.exe and a false file called crypted.vol that contained random characters. For the USB to call home via a DNS request the human actor had to run the encryptor.exe and attempt a password.

4. RESULTS AND DISCUSSION

The extensive data from the testing are still being analysed however the following statements put the extent of the exposures uncovered in perspective for the purposes of the discussion.

- All organisations were readily and easily enumerated with only 2 organisations being aware of the probing.
- All organisations had significant exposures uncovered in the network scanning and testing.
- All except one of the organisations detected the intense scans and attacks of the system.
- All except one of the organisations did any tangible, credible and trackable escalation of incidents.
- Some of the organisations logging and record keeping is that poor that no evidence could be located post testing.
- Only one organisation was not compromised by USB stick attack. Two external IT providers to the organisations were also compromised.
- All USBs were effective within less than 48 hours of being dropped at the organisations.

4.1 Escalation and responses or lack thereof

All organisations showed no or extremely poor escalation of incident to authorities. Only two of the 15 organisations escalated the attacks to authorities for further investigation. This is alarming in that 13 organisations failed to detect and effectively respond to sustained attacks on their systems.

To their credit, two organisations provided some response but again there are concerns in their level of response. One organisation undertook what can be best described as multiple agency contact, basically contacting anyone who would listen. This mass alerting was conducted against the organisations policy which had a person in a designated position would make the call and then only to one agency. This demonstrates poor organisational awareness of policy, which may indicate a lack of training or familiarity with escalation.

Another organisation had succumbed to crying wolf or demonstrated Hawthornian effects in response, such that they were contacting agencies and reporting attacks from the attack team when in fact they had been idle on that organisation for 10 days. Basically, other IPs that were actually attacking from a home based DSL account within the Western Australian ISP IP address spaces were being attributed to the attack teams efforts and escalated to responder agencies.

An intentional ruse was effective in that while attacking with the home based DSL accounts simultaneously high intensity attacks and probes were being perpetrated from the large bandwidth virtual server accounts with no reporting of these apparent by any of the responding organisations.

Feedback from responder agencies has been that escalation and reporting was inadequate and presented no real opportunity for defending systems. In particular one responding agency has resolved to undertake an education and advice program to inform operators how best to report a cyber attack in order to get resolution of the attack.

4.2 Technology tokenism

Some of the organisations had expensive dedicated security appliances that were deployed and inadequately managed, which indicates these organisations are suffering from technology tokenism. It could be that staff were not trained in the use of these appliances, which indicates strongly that organisations should look at the total investment cost which includes ongoing training and support for staff. Also, many of the network borne threats are complex, multi-partite and asymmetric. The modern security appliance is a highly complex system and needs constant adjustment to get optimal performance from it.

4.3 Security is so inconvenient

IT Staff from several organisations reported a lack of acceptance or recognition of risk in IT systems by upper management. One organisation relayed that they had in fact tried to secure USB ports by disabling them through policy management afforded by Windows XP. Soon after deployment was enacted they were summarily told to undo this by top line management as it was not convenient and USB posed no real threat or risk to the organisation. There were also similar vignettes communicated where executives was not aware of or did not want to acknowledge the clear and present danger that not deploying or enabling security measures brought to the organisation.

4.4 Post incident forensics

Another stage of this activity is the investigation of post incident ability to respond to evidentiary requirements and also provide data for analysis of incidents. The analysis of any log files or intrusion data is not yet complete however there have been uncovered significant issues already in this phase.

Several of the organisations have not been able to provide any tangible log file data. There are several reasons, the most alarming is that preservation of log files is not occurring beyond a short time window of a week to a few days dependant upon logging activity i.e the log files are live and simply utilise fifo. There is no daily archiving or storage of log data in these organisations, which under WA state law is a breach of the State Records Act, let alone the fact its basic security practice. Any argument that storage space or performance of appliance is a significant issue is a very tired IT industry meme. Hard disk storage is incredibly cheap and devices are sufficiently powerful that any logging is now in the realms of 1-2 per cent of CPU and if an IPS or device is that marginal bigger issues are afoot.

Several of the organisations do not know how to extract data from their IDS/IPS, firewall systems when this information was requested they have supplied HTML documents taken from their system management consoles. This is clearly an inadequate response.

4.5 Penetration Testing vs. Vulnerability Assessment

Of concern is that nearly all organisations examined in this research had recently paid external companies to conduct penetration tests against their infrastructure. The evidence presented as a result of examining these 15 organisations is that penetration testing seems to have almost zero value, whilst having a very high cost, both in monetary and security terms.

The profile of companies employed to conduct such penetration testing are commonly audit organisations for which their major business is financial audit. However, the growth in the use of the internet for e-commerce and other core business functions has seen these organisations branch out into IT security auditing, or so called ethical hacking. As such, when an organisation requests an external audit of their organisations, an evaluation of the health of general computer controls as they relate to financial system access is also conducted. Increasingly, organisations are also being sold ethical hacking or penetration testing in relation to their internet facing infrastructure. In addition to being part of a financial audit, organisations are also using these same audit firms to conduct ad-hoc assessment of their network infrastructure as part of change management or configuration changes.

There are anecdotal reports from some organisations that the companies conducting these tests commonly ask them to add them to a firewall or IPS white list or to turn off certain security features so that they can conduct the test. Such an approach may allow for testing of an individual component with a companies defence infrastructure, but it certainly does not test or evaluate the security of an organisation as a whole. Standard practice for such organisations is to use recent graduates armed with a tool (commonly Nessus and Nmap) to run scans against the target organisation who requested the test. Whilst the people using the tools may have been adequately trained and instructed, they are far from network security experts, or even ethical hackers, as they sometimes refer to themselves.

In defence of the audit organisations, they are likely only providing the service which they are asked to perform. That is, organisation A asks for, and receives a penetration test of their firewall. Is this a useful test of organisation A's security? No, but it is what they requested. Having said that, there appears to be an ethical issue in relation to charging large amounts of money for a test which is largely worthless, regardless of whether the organisation specifically requested it or not.

Of far greater value to an organisation is a vulnerability assessment which assesses the overall security posture of an organisation, including such aspects as policy, procedure, physical security, change management and governance. For example, a penetration test may find an open port on a firewall that should have been closed. In that instance, the recommendation is to close the port. A vulnerability assessment, through an examination of the firewall rule sets, would also pick up that a port was open. However, the recommendation would then be to look at change management and policy and procedure in relation to network security as to *why* the port was open, and to prevent such an issue occurring in the future.

5. CONCLUSION

This engaged research has resulted in uncovering significant issues that need addressing in organisations with respect to preparedness to attack, response, escalation and investigation of external attack of cyber systems.

All of these organisations have an IT department and in some cases have personnel responsible for security which mitigates the resourcing defence that many organisations put forward, some also outsource their daily IT security to specialist firms. Many have also paid large amounts of money to external audit agencies to conduct penetration tests against their infrastructure. However in defence of the IT staff in these IT departments often security of systems is compromised by poor management decisions as result of poor understanding of IT based risk. This is all too a common theme in investigations of this sort and something both sides of the IT management divide need to work on.

There was largely systemic failure to detect and respond to the attacks. Only 2 out of the 15 organisations provided any semblance of coherent response to the attacks, the other 13 can only be categorised risk wise as extreme. The work has uncovered that there is significant fundamental work that needs to be undertaken in these organisations before any semblance of an IT security posture or awareness could be proclaimed.

6. REFERENCES

Fyodor. (1998). "Remote OS detection via TCP/IP stack fingerprinting." Retrieved 10 May, 2002, from http://www.insecure.org/nmap/nmap-fingerprinting-article.txt.

Scarfone, K., Souppaya, M., Cody, A. & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology. Gaithersburg, Maryland

Sullo, C. and D. Lodge (2011). Nikto2.