Use the PCAP files to see/identify traffic

Have a Linux guru on the team

Public – non-routable addresses. DMZ –

All machines have their addresses translated – whether they have the DNS working and correct – so our students used the Public DNS.

Patching – some supported repos – define or do version upgrades – pain –

For each system for windows 8.1 search for CVEs – search for vulnerabilities. Want to take care of the remote code executions. Specifically patch for those CVEs.

Splunk – whether inline or passive monitoring

Phantom 4.1.94 – if a CVE that is remote code execution –

2008 R2 – have Metasploit modules for them.

OSCP – learn the methodology.

If Metasploit module for them – patch them first. Work arounds – shut off the services and make config and registry changes – a lot of registry changes in Windows 7 and above to protect against vulnerabilities.

Once tighten up the security then best practice and monitoring.

Update PHP – sometimes update to an incremental then check the updates for CVE vulnerabilities.

Server 2012 – doesn’t need a bit of incremental. Many want to find the CVEs.

Best Practice hardening Windows 8.1 – Hardening CentOS, Hardening Fedora 21. With Windows.

IoT – check to see what and look for default password and things.

If they want to script the stuff – if services need to be stopped let each other know. Reboots are an issue. Set people as a priority – who owns which system and who is going to reboot – have a checklist for who is securing and have that person responsible.

Saving .conf files – have them backup and stored securely – and have passwords changed.

If management tells you to change something on the root server in the web – make sure you have backups and what you are changing doesn’t break something.

CVEs and fix the remote code – reflected cache and things around those lines. They may try to Man-in-the-Middle – if a small vulnerability if it is using a weak version of encryption someone may be able to listen. Have a Gantt chart – have an owner. If someone has something – a version may break something – talk to the others to see what it may break. Database will default – mail will turn on forwarding.

Look into what the full services are – go to the vulnerability list and see what the people focus on. Web interface – file inclusion – get the services patched – the 10 vulnerabilities. A lot of them are listed in CVE remote code executions. A couple of them do not have a system exploit. If it requires memory relocation. If familiar with the methods.

Service enumeration – host enumeration – if honeypot could watch the attackers. With Palo Alto make every IP address respond to would make them work on scanning everything.

Windows – if they allow you to load – Bit9 can be loaded. Require the red team to pack the payloads – if you can protect the quick and dirty then they will need to go to deeper tactics.

Don't worry so much of monitoring the system – get updates and CVEs and be careful what you log into with what accounts – change your password after the hour starts. Mimikatz – they will pop one of the boxes – have unique

Whatever chat programs you are using – if you can communicate out of band.

Move files back and forth – pull the management requests down early – with some patches you could use them on multiple systems. Same path vulnerabilities – make sure all the file sharing is locked up.

Advanced IP Scanner – less intrusive scanning. Your own monitoring. If you have the static IP – do continuous pinging for the static addresses– if it has the web interface will have a nice mapping.

Checklists – CVE's patch remote code execution and reflected cache. Add firewall services – do a lot with command-line. IP tables – lock them down a little more.

Scanned for web interfaces – use Burpsuite to scan the web services. – Advanced IP Scanner – any with Web Interfaces – run Burpsuite – to find Cross-Site Scripting, SQL injection.

As Soon as they are done checking services they are going to go to the Web Interfaces – make sure all CVE's on that are patched.

Check for Fuzzing.

Bit9 – load a SIM and basic attacks won't be able to take over. Put Bit9 and they will need to run Advanced Persistence Threats to come through the systems.

Be strategic with the updates. Take care of the top 3 CVEs. If run the update will take the system down.

Easy for in a Windows – someone doing a drive by and can download a file.

Set all of the default browsers to the latest version of Google Chrome and throw Ad-Blocker on there. Some drive-by attacks – check for Java and Flash and remove.

If you need to download on the 2008 Server – most servers are locked down. Server – is going to be a bit more restrictive then the Windows 8.1 – so download on the 8.1 and send securely to the Server 2008 R2.

Look at how LDAP integrates with the environment. Have Exchange and LDAP on the Windows Server 2008 R2.

PS.exe going to want to remove those – check out Mimikatz and ps.exe – close those ones. Look for CVEs for the Ubuntu 12.

for the Linux/Unix – get the preliminary patches done – 1 by 1.

Python scripts or better methods. With the ways the packet management works you can script them. Patches and dependencies.

Remote services – monitoring services – trick them into thinking they are monitoring and make them think things are still monitoring –

Splunk/Phantom

Windows Server/8.1

FTP Web – if not needed turn off.

Most of the systems us salted and hashed passwords for these systems. The windows NTLM hashes are easy to crack. A good system can crack the password in a matter of minutes.

Throw a honeypot on the Internet to check for vulnerabilities.

Reflected DNS attacks – if they are doing a full distributed denial of service.

Verify the accounts they say they have – look at the other accounts – modify the password and permissions. Do password changes on the Admin and System Accounts – have new users created if possible.

Bit9 Demos – professional versions – Set-up your own domain and email and ask for a 30 day trial. Nessus is $2400 a year.

Nmap – Zenmap might be a little bit different. Script it all and have it done in the first 30 minutes. 7.zip the scripts inside of an encrypted file. Pack the scripts into something else. Some of the GIT repos – if you can't patch there are registry hacks and can registry hack into non-existence. Day 1 or zero day individuals had methods of patching before Windows.

Use key words to narrow the CVE search based on the OS version. CVE 2017 100354 is this something we need to patch right away. Patch in 2015. Sometimes by patching a vulnerability you can patch a few different vulnerabilities.

Slow them down from exploiting the firewall – show run config on the router – find out the version and see if there is anyway to slow them down. Change the size of the buffer in memory – make it a longer password or a password with spaces in it. Might be little things that the guys can take to slow them down.

Keep them out of the firewall that would be amazing.

Firewall has known vulnerabilities – run CVEs on the firewall. Check in the competition and see if they can patch the firewall – or fix the CVEs. If have a firewall they should be safe but if they have back doors on the system – look for anything calling out from the firewall.

Reason they have the splunk is to catch those things IRC or command and control systems.

Palo Alto – admin services only for internal stuff. If you can enforce there is not method they can use to get into your system.

If teamview you can fix DNS queries so they are not able to access the Teamview.

1. Fix any remote executions
2. OWASP Top 10 for those years – the years of the Cent OS systems
3. Configuration changes on the firewall – might be enough to keep the people out.
4. If can't patch – change password every minutes
5. Within an hour you can patch the Palo Alto firewall – do the configuration changes
6. Look at what's calling home – look at DNS requests that are out of order
7. Midterpreter session or reverse shell – using them to all home.
8. Windows framework dependencies
9. Get Bit9 located on the Windows Server – social engineering to a Sales person.
10. 30 Day trial – registered email address.
11. The second that buffer overflow happens Bit9 will detect the code and stop it from running.
12. SIEM – if report and block – pentests are annoying – pack the payload or change the fingerprint – to get around the SIEM.
13. Backup the configurations – don't want to break the systems.
14. Privilege escalations – for each operating system read the best practice
15. Also watch youtube for hardening.

16. Look at processes to see what is running. Look at the logs that you have.
17. After that have a game plan of who owns those systems.
18. OS top ten – back them.
19. With a PA if you continuously change the password or make the admin interface internal only it will change the attack strategy.
20. Read PCAP files – practice digging into the PCAP files –
21. How about TCP Dump with the PCAP files – for the Linux systems.
22. Write down dependencies – if there is a CVE patch but it requires a GUI or another program – get it written down. Repetition is the best way.
23. If you want to work in an environment – practice every day – complete a lab a day – then you will become "billable".
24. Metasploit – Mimikatz – ps.exe – need to know how they work to defend them.
25. Sometimes it is a simple as editing the registry but then other times it is not.
26. Don't reuse passwords or iteration of a password.
27. Programming – pix assembly, x86 assembly, arm assembly, thumb assembly, C++, C python.
28. The ability to do exploit development in assembly – and will make you a better C programmer. You will feel confused and not want to continue but keep at it. Google what to know about C.
29. May be confusing but after awhile will be confused.
30. Open source VLC video streaming app.
31. Can add information into the p-frame add data back in for the p-frame. Think I have watched a couple jeopardy reruns that may have injected code into the p-frame.
32. Gibson Assembly Language http://www.naspa.net/magazine/2005/0905/T0509009.pdf
33. DOS 3.2 source code is all open now.
34. Tools that only work on Linux – so in addition to programming become very comfortable with Linux. Installing software – dependencies – compiling source code.
35. PMP – SCRUM master project manager knowledge is a good skill. SANS offers a project management for Pentesting. Statements of Work – RFPs – how to quote a Pen test.

Game Plan or Playbook!

One other thing – I was thinking is Incident Response Report.

He recommends – programming an hour a day and reading the pcap and CVE files.

If any questions in general

westen.hecker@gmail.com or Linked In https://www.linkedin.com/in/weston-hecker-60ab3076